O papel das Relações Públicas na gestão de ciberataques:

Proposta de um guia para preparação estratégica das organizações no contexto português

SARA ALEXANDRA GASPAR ANTUNES

DISSERTAÇÃO SUBMETIDA COMO REQUISITO PARCIAL PARA OBTENÇÃO DO GRAU DE MESTRE EM GESTÃO ESTRATÉGICA DAS RELAÇÕES PÚBLICAS

Orientador:

Professor Doutor Nuno da Silva Jorge

Escola Superior de Comunicação Social

ABRIL 2024

DECLRAÇÃO ANTI-PLÁGIO

Declaro ser a autora da presente dissertação, parte integrante das condições exigidas para a obtenção do grau de Mestre em Gestão Estratégica das Relações Públicas. Declaro, ainda, este ser um trabalho nunca submetido (no seu todo ou em qualquer uma das suas partes) a outra instituição de ensino superior para a obtenção de um grau académico ou outra habilitação. Todas as citações estão devidamente identificadas. Mais acrescente que tenho consciência de que o plágio é crime e que poderá levar à anulação do presente trabalho.

Lisboa, abril de 2024

Sara Antunes

Sara Antunes

Agradecimentos

A conclusão desta dissertação muito se deve ao apoio incondicional de todos aqueles que me acompanharam ao longo desta jornada e, por esse motivo, não podia deixar de manifestar o meu profundo agradecimento pelo incentivo, inspiração e motivação diária que me ajudaram a concretizar um dos principais objetivos da minha vida.

Ao meu orientador, o professor Doutor Nuno da Silva Jorge, por me ajudar a delinear este projeto, sempre com a certeza de que estava no caminho certo e fazendo-me acreditar no meu potencial. Pela motivação, disponibilidade e por todas as sugestões que enriqueceram este estudo, obrigada!

A todos os profissionais entrevistados que, sem exceção, manifestaram total disponibilidade, empatia e interesse em colaborar no desenvolvimento desta dissertação, constituindo um contributo fundamental para a obtenção dos meus resultados. Um leque diversificado de perspetivas e experiências que, inevitavelmente, me enriqueceram a mim também!

Aos meus colegas de mestrado, em especial, àqueles que privaram comigo e com os quais estabeleci uma ligação forte de amizade, por toda a motivação, apoio e espírito de entreajuda. Tenho a certeza de que, juntos, conseguimos chegar mais longe!

Ao meu núcleo de amigos da licenciatura que, embora tenham seguido diferentes rumos de vida, estiveram sempre presentes e continuaram a ser um pilar fundamental na minha vida. Sem o vosso apoio incondicional, este percurso teria sido muito mais complicado!

Aos meus amigos mais próximos – de infância, da Ericeira e que serão para a vida –, pela compreensão nos momentos em que não conseguia estar presente, por acreditarem que o retorno do meu esforço estaria para breve e, acima de tudo, por confiarem no meu potencial – muitas vezes mais do que eu própria. Levo-vos para sempre comigo!

E, por fim, à minha família pelo maior apoio de sempre! Em especial, aos meus pais, ao meu irmão e aos meus avós, o meu verdadeiro porto seguro, por estarem sempre presentes, por nunca me permitirem desistir e por me incentivarem a concretizar os meus sonhos – sem vocês, nada disto seria possível! A todos os amigos de longa data, que se tornaram família para nós, obrigada pela motivação, por todos os conselhos e por acreditarem tanto em mim. Sei que esta conquista é, em parte, vossa também!

Resumo

Perante o aumento significativo das ciberameaças, as organizações enfrentam cada vez mais problemas ao nível da segurança dos seus sistemas e redes informáticas, o que exige um maior nível de prevenção e gestão de crise que lhes permita recuperar eficazmente do incidente, mitigar eventuais danos e assegurar a reputação organizacional. Neste sentido, a presente dissertação procura estudar a prevenção e resposta a um ciberataque, aplicadas em particular ao contexto português, e compreender a importância de as organizações estarem devidamente preparadas para a eventualidade de um incidente deste género.

O principal objetivo deste estudo consiste na apresentação de uma proposta de Guia de Boas Práticas de Prevenção e Resposta a um Ciberataque, que sirva não só de inspiração a todos os interessados no tema em questão, mas que se constitua, também, como uma importante ferramenta para os profissionais de Relações Públicas das organizações portuguesas utilizarem no processo de prevenção e preparação da resposta a um ciberataque. De forma prática, pretende-se clarificar a importância da atividade de Relações Públicas na gestão de um ciberataque.

Além do importante contributo das evidências teóricas constatadas na revisão da literatura, este guia foi construído tendo por base a perspetiva de diferentes profissionais e especialistas relativamente à importância da prevenção e resposta a um ciberataque, bem como acerca das principais medidas e ações de segurança e comunicação a implementar pelas organizações num incidente deste tipo.

Os resultados evidenciaram que é possível as organizações serem alvo de um ciberataque e, ainda assim, recuperar do incidente com o mínimo de danos possíveis e manter a sua reputação. Não obstante, é necessário existir um esforço permanente da organização no que toca à gestão do ciberataque, destacando-se o papel fundamental do profissional de Relações Públicas na resolução do incidente.

Palavras-chave: Cibersegurança; Relações Públicas; Reputação; Gestão de Comunicação de Crise; Boas Práticas

Abstract

Given the significant increase in cyber threats, organizations are facing more and more problems in terms of the security of their computer systems and networks, which requires a higher level of prevention and crisis management that allows them to recover effectively from the incident, mitigate any damage and ensure organizational reputation. In this sense, this dissertation seeks to study the prevention and response to a cyberattack, applied in particular to the Portuguese context and to understand the importance of organizations being properly prepared for the eventuality of an incident of this kind.

The main objective of this study is to present a proposal for a Best Practices Guide for Preventing and Responding to a Cyberattack, which will not only serve as inspiration for all those interested in the subject in question, but will also be an important tool for Public Relations professionals in Portuguese organizations to use in the process of preventing and preparing a response to a cyberattack. In a practical way, the aim is to clarify the importance of Public Relations in the management of a cyberattack.

In addition to the important contribution of the theoretical evidence found in the literature review, this guide was built based on the perspective of different professionals and experts regarding the importance of preventing and responding to a cyberattack, as well as the main security and communication measures and actions to be implemented by organizations in an incident of this type.

The results showed that it is possible for organizations to be the target of a cyberattack and still recover from the incident with as little damage as possible and maintain their reputation. Nevertheless, there needs to be a permanent effort on the part of the organization to manage the cyberattack, highlighting the fundamental role of the Public Relations professional in resolving the incident.

Keywords: Cybersecurity; Public Relations; Reputation; Crisis Communication Management; Best Practices

Índice

Índice de Figuras

Índice de Tabelas

Introdução

Ao longo dos últimos anos, a cibersegurança tem vindo a ganhar cada vez mais relevância na vida das pessoas, das organizações e da sociedade como um todo (Centro Nacional de Cibersegurança, 2023, p. 8). A cibersegurança tornou-se, inclusive, uma das áreas de atenção prioritária tanto para os governos, como para as empresas (Carballo-Cruz, 2022, p. 24).

Atualmente, o ciberespaço constitui-se como um imperativo fundamental e integral de qualquer negócio, pelo que a cibersegurança deve ser integrada na estratégia empresarial de todas as organizações, estabelecida como um fator determinante para o seu sucesso (Deloitte, 2022, p. 8). Esta é uma necessidade crescente que decorre do aumento significativo do número de ciberataques nos últimos anos.

Segundo o Relatório Semestral de Cibersegurança de 2023 da Check Point, as atividades criminosas intensificaram-se no primeiro semestre do ano, com um aumento de 8% nos ciberataques semanais globais a decorrer no segundo trimestre, registando o valor mais elevado dos últimos dois anos (Check Point, 2023b, p. 4). Durante o referido semestre, Portugal registou uma incidência de 11 empresas atacadas, o que representa uma estabilidade no número de ataques em relação ao semestre anterior (S21sec, 2023, p. 9). Ainda assim, importa destacar 2022 como um dos anos, desde que há registos, com o maior número de ciberataques de grande impacto social e nas infraestruturas e serviços em Portugal, tendo como resultado uma grande visibilidade do tema na opinião publicada (Centro Nacional de Cibersegurança, 2023, p. 7).

Perante este cenário, é urgente as organizações aumentarem a sua resiliência e capacidade de resposta a um ciberataque, fundamentada num equilíbrio entre a mitigação e recuperação dos sistemas e a gestão de comunicação do ciberataque (Narendra, 2022). Embora seja um assunto ainda com reduzida expressão na literatura portuguesa, a comunicação em situação de ciberataque começa a ganhar relevância e a equiparar-se à importância da gestão do próprio incidente (Sapriel, 2021, p. 2).

Sendo a reputação de uma organização um recurso valioso ameaçado por crises (Coombs & Holladay, 2002, p. 167), é cada vez mais importante as organizações compreenderem a importância de prevenir e responder eficazmente a um ciberataque, não só para recuperar o mais rápido possível do incidente, mas sobretudo para garantir a manutenção da sua reputação junto dos *stakeholders*.

Não obstante, Lino Santos, coordenador do Centro Nacional de Cibersegurança, acredita que, embora exista atualmente "uma maior consciência dos gestores e das organizações que tratam dos nossos dados pessoais", a verdade é que "temos os incidentes a acontecer e temos as empresas com um grau de preparação ainda insuficiente para lidar com este tipo de situações" (Santos in Mesquita, 2022). O certo é que "há uma diferenciação significativamente positiva entre entidades que tendo sido atacadas recuperaram num tempo finito e recuperaram o negócio […] As outras, que estavam menos preparadas, demoram muito tempo, podem nunca voltar ao estado em que estavam e perdem informação para sempre" (Marques in Caçador, 2022a).

É neste sentido que, face a uma realidade que afeta cada vez mais organizações e perante um cenário de insuficiente preparação das organizações portuguesas, se revela pertinente estudar a prevenção e resposta a um ciberataque, aplicadas em particular ao contexto português, e compreender a importância das organizações estarem devidamente preparadas para a eventualidade de um incidente deste género. Dado o crescimento significativo de casos de ciberataque a ocorrer em Portugal, sobretudo a partir de 2020 (Centro Nacional de Cibersegurança, 2023, p. 26), é possível entender que o presente tema se constitui como um *hot issue*, com cada vez mais expressão na agenda mediática portuguesa e que tem vindo a criar *buzz* entre empresas e investigadores.

Posto isto, a ideia explorada neste enquadramento materializou-se na seguinte pergunta de partida:

"Como é que os profissionais de Relações Públicas podem contribuir para a preparação das organizações em situação de ciberataque, no contexto português?"

Por forma a responder de forma completa e eficaz à pergunta de partida, foram estabelecidos os seguintes objetivos específicos de investigação: 1) Desenvolver um quadro teórico sobre Cibersegurança no contexto das Relações Públicas em Portugal; 2) Compreender a perspetiva de profissionais de Relações Públicas sobre o papel que desempenham numa situação de ciberataque; e 3) Elaborar uma proposta de guia de boas práticas de prevenção e resposta a um ciberataque a implementar pelos profissionais de Relações Públicas nas organizações. Significa isto que os resultados e conhecimentos adquiridos ao longo do presente estudo culminam numa proposta de Guia de Boas Práticas de Prevenção e Resposta a um Ciberataque baseado não só em evidências teóricas, como na experiência e perspetivas de diferentes profissionais e especialistas na área da Cibersegurança e na área das Relações Públicas.

Para dar resposta aos objetivos de investigação e poder contribuir para a construção do guia de boas práticas, revelou-se necessário abordar alguns conceitos fundamentais. O Capítulo I inicia-se com o estudo da reputação e comunicação de crise no âmbito das Relações Públicas. Para o efeito, começou por se abordar o papel estratégico das Relações Públicas, procurando explorar em profundidade a ambiguidade na definição do conceito, a sua institucionalização enquanto atividade de gestão estratégica, os quatro modelos pioneiros na área e as diferentes perspetivas e paradigmas acerca da prática de Relações Públicas. Segue-se uma análise sobre a reputação enquanto ativo fundamental para o sucesso organizacional, que inclui uma explicitação acerca da complexidade de institucionalização do conceito, do seu valor no seio das organizações e da integração dos conceitos de identidade e imagem no processo de construção da reputação organizacional. Por último, apresenta-se uma reflexão acerca da importância da comunicação no processo de gestão de crise, através do esclarecimento da interpretação do conceito de crise à luz da perceção dos *stakeholders*, da necessidade de comunicação de crise para uma eficaz gestão de crise, das diferentes fases de gestão de uma crise e, ainda, das teorias que defendem um impacto da comunicação de crise no comportamento do público.

No que se refere ao Capítulo II, este aborda o fenómeno dos ciberataques enquadrado na área das Relações Públicas. O capítulo inicia-se com uma análise acerca da emergência da Cibersegurança enquanto preocupação atual nas organizações, em que é abordado o conceito de Cibersegurança, o seu contexto histórico, o enquadramento legal – seja a nível internacional, europeu e nacional –, o papel do Estado, as entidades com autoridade em matéria de Cibersegurança, a importância da Cibersegurança, as vulnerabilidades e ataques informáticos, alguns casos de ciberataque a nível nacional e internacional, as medidas de prevenção e defesa e os desafios, ameaças e tendências atuais na área. Por fim, numa ótica de convergência entre as duas áreas, apresenta-se o estudo da comunicação de crise em contexto de ciberataque e o seu impacto na reputação organizacional.

Após a revisão da literatura, surge a explicitação acerca da abordagem empírica adotada no presente estudo – Capítulo III. Optou-se pela adoção da metodologia qualitativa, através da realização de entrevistas a profissionais e especialistas tanto da área da Cibersegurança, como da área das Relações Públicas. Por forma a analisar corretamente os dados obtidos nas entrevistas, procedeu-se à análise de conteúdo qualitativa.

No Capítulo IV, surge a apresentação e interpretação dos resultados. Numa primeira instância, apresentam-se os resultados relativos às entrevistas realizadas aos profissionais e especialistas em Cibersegurança, resultando no estudo da Cibersegurança no contexto português.

De seguida, apresentam-se os resultados relativos às entrevistas realizadas aos profissionais e especialistas em Relações Públicas, que culmina no estudo da comunicação de crise em situação de ciberataque. O capítulo finaliza com uma breve explicitação acerca do guia de boas práticas, sobretudo no que respeita à sua definição, a quem se destina, o seu principal objetivo, o seu valor e como está organizado.

A dissertação finaliza-se com a apresentação de uma proposta de Guia de Boas Práticas de Prevenção e Resposta a um Ciberataque, que reúne as mais importantes evidências teóricas abordadas na revisão da literatura, bem como as perspetivas dos entrevistados. Espera-se que este guia seja um contributo importante não só a nível académico, mas sobretudo a nível organizacional, aconselhando as organizações portuguesas através de um conjunto de recomendações de prevenção e resposta a um ciberataque, no sentido de garantir uma melhor recuperação do incidente e a manutenção da reputação organizacional.

Capítulo I – O estudo da Reputação e Comunicação de Crise no âmbito das Relações Públicas

1. As Relações Públicas enquanto processo estratégico de comunicação

1.1. Relações Públicas: a ambiguidade na definição do conceito

Atualmente, as Relações Públicas posicionam-se como uma disciplina institucionalizada e com a discussão sobre a sua definição como ultrapassada, embora o seu processo de institucionalização não tenha sido consensual.

Desde o início da sua institucionalização como prática moderna, as Relações Públicas sofreram uma crise de identidade – em grande parte da sua própria autoria (Hutton, 1999, p. 199). Tanto do ponto de vista teórico como prático, as Relações Públicas não conseguiram estabelecer uma definição amplamente aceite em termos do seu propósito fundamental, da sua metáfora dominante, do seu alcance ou das suas dimensões subjacentes (ibidem, 1999, p. 199). Embora alguns autores tenham apresentado noções claramente articuladas sobre a natureza e o propósito do campo das Relações Públicas, parece ter havido poucos progressos na forma de consolidação e desenvolvimento dos seus princípios básicos, resultando na associação da atividade a uma variedade de denotações e conotações, na sua maioria negativas (ibidem, 1999, pp. 199-200).

Para muitos, as Relações Públicas são percecionadas como uma atividade de mensagens cujo principal objetivo é fazer com que as organizações tenham uma boa imagem nos meios de comunicação social (Grunig, 2011, p. 12). Bernays (1923/2015) reforça esta ideia, ao afirmar que, por vezes, os profissionais de Relações Públicas são associados aos termos "propagandista", "agente de imprensa" ou "publicitário", embora esta desaprovação da atividade se baseie em nada mais substancial do que impressões vagas (pp. 34-35).

Em certa medida, o número e variedade de definições apresentadas por académicos e profissionais de Relações Públicas é legítima, dada a história relativamente curta da área como prática moderna e a sua tendência natural para se adaptar a um ambiente empresarial em constante mudança (Hutton, 2007, p. 51). Tal como reforçam Tench e Yeomans (2009), as Relações Públicas são utilizadas numa vasta gama de indústrias e em cada uma delas surgiram aptidões e competências ligeiramente diferentes entre os profissionais (p. 4). Não obstante, o crescimento e a diversificação do corpo teórico têm contribuído para um maior reconhecimento das Relações Públicas não só como disciplina, mas também como profissão (Sebastião, 2012, p. 25).

No sentido de clarificar a razão para a existência desta ambiguidade na definição do conceito de Relações Públicas, Verčič *et al.* (2001) esclarecem que, além da diferença cultural, a

diferença de idiomas e consequente tradução do termo resultam em diferentes interpretações do conceito (p. 376). A título exemplificativo, no caso da língua alemã, o termo "relações públicas" significa "obra pública", sendo caracterizado por "trabalhar em público, com o público e para o público", contrariando a clássica definição americana que entende o conceito como a gestão de relações entre uma organização e os seus públicos (ibidem, 2001, p. 376). Contudo, um dos principais problemas reside no facto de, em muitas línguas europeias, simplesmente não existir uma tradução adequada para o termo "relações públicas" e, por esse motivo, utilizam-se diversas definições como "gestão da comunicação", "comunicação corporativa" ou "comunicação aplicada" (ibidem, 2001, p. 379).

O facto de não se chegar a um consenso acerca da definição do conceito de Relações Públicas resultou em confusão, perda de credibilidade, perda de influência e perda de responsabilidades-chave para outras áreas funcionais (Hutton, 2007, p. 61). Por forma a resolver tais problemas, as Relações Públicas devem adotar para si próprias uma definição e um paradigma de organização a longo prazo, substantivo e consensualmente aceite, procurando melhorar significativamente o seu conhecimento acerca de ambos os elementos-chave do conceito – relações e gestão –, assim como abandonar a ideia de que a comunicação é o único fator determinante (ibidem, 2007, pp. 56-61).

1.2. A institucionalização das Relações Públicas enquanto atividade de gestão estratégica

O termo "relações públicas" remonta ao século XVIII, em que o seu significado começa a ser entendido como uma relação formal entre organizações, países e pessoas (Myers, 2021, p. 6). De facto, nos anos que precederam e durante a Primeira Guerra Mundial, o termo "relações públicas" era muito utilizado na indústria dos serviços públicos. Nessa altura, o seu significado era quase idêntico ao atual – uma relação formal entre uma organização e os seus vários públicos (ibidem, 2021, p. 6). Já em meados do século XX, o termo profissional de relações públicas tornou-se um nome mais padronizado para aqueles que praticavam a atividade, começando a dar os primeiros passos na consolidação do seu corpo teórico (ibidem, 2021, p. 6).

Não obstante, importa mencionar o contributo de dois nomes de elevada importância na história das Relações Públicas: Ivy Lee, habitualmente considerado o pai histórico das Relações Públicas, e Edward Bernays, conhecido como precursor na procura de uma fundamentação científica das Relações Públicas (Gonçalves, 2010, p. 31).

Uma das iniciativas-chave da política de Ivy Lee, que ficou marcada na história das Relações Públicas, é a "Declaração de Princípios" (1906), fundamentada na máxima "The public

be informed", tendo por base o estabelecimento de relações comunicacionais assentes em valores como correção, credibilidade e equidade (Gonçalves, 2010, p. 32). Aliada a esta iniciativa, Ivy Lee introduziu a "política de portas abertas", passando a ser concedida aos jornalistas a oportunidade de visita a locais outrora completamente interditos, como fábricas ou locais de acidentes (ibidem, 2010, p. 32). Para Ivy Lee, as atividades de Relações Públicas não passaram de uma série de eventos de curto prazo para atrair publicidade e fazer cumprir um objetivo específico, enquanto Bernays, influenciado pelas teorias psicológicas do seu tio, Sigmund Freud, procurava teorias mais profundas e uma certa compreensão sobre como controlar e influenciar o público (Butterick, 2011, p. 9). Tendo por base a premissa de controlo da opinião pública, Bernays (1923/2015) acredita que o público exige cada vez mais informação e espera ser aceite como júri em assuntos que têm uma grande importância pública (p. 46).

Em 1976, numa tentativa de esclarecer o conceito de Relações Públicas, Harlow reuniu 472 definições e chegou à conclusão de que não existia uma definição consensualmente aceite como referência para todos os interessados em Relações Públicas (p. 36). É neste sentido que propõe a sua própria definição do conceito:

> *As relações públicas são uma função de gestão distinta que ajuda a estabelecer e manter linhas mútuas de comunicação, compreensão, aceitação e cooperação entre uma organização e os seus públicos; envolve a gestão de problemas ou questões; ajuda a gestão a manter-se informada e a responder à opinião pública; define e enfatiza a responsabilidade da gestão em servir o interesse público; ajuda a gestão a manter-se a par e a utilizar eficazmente a mudança, servindo como um sistema de alerta precoce para ajudar a antecipar tendências; e utiliza a investigação e técnicas de comunicação sãs e éticas como as suas principais ferramentas* (Harlow, 1976, p. 36)

Embora a harmonia em torno da definição do conceito se tenha revelado um problema, existe um consenso na definição das Relações Públicas enquanto função de gestão da comunicação entre uma organização e os seus públicos, que estabelece e mantém entre eles relações mutuamente benéficas (Broom & Sha, 2013, Grunig & Hunt, 1984; Hutton, 1999). Segundo Hutton (1999), "gerir relações estratégicas" oferece uma definição parcimoniosa de Relações Públicas que é facilmente comunicável, relevante tanto para a teoria como para a prática e não tão ampla a ponto de ser desprovida de sentido, nem tão estreita a ponto de ser excessivamente limitativa (p. 211).

Numa abordagem semelhante, o *Institute of Public Relations* definiu, em 1987, as Relações Públicas como sendo "o esforço planeado e sustentado para estabelecer e manter o entendimento entre uma organização e os seus públicos" (Theaker, 2012, p. 5).

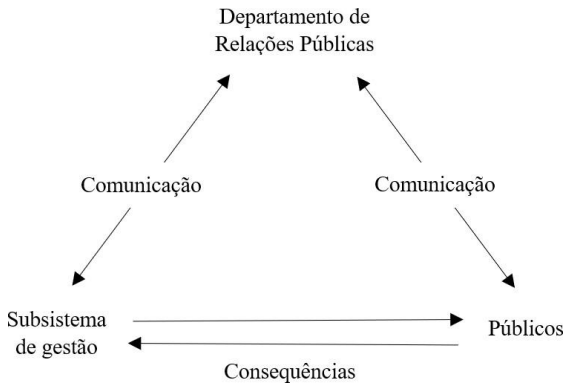
Segundo Botan e Taylor (2004), a tendência mais marcante na fase de institucionalização das Relações Públicas é a sua transição de uma perspetiva funcional para uma perspetiva que se centra na comunicação como um processo de criação de sentido (p. 651). Por um lado, a perspetiva funcional, prevalecente nos primeiros anos da área, perceciona o público e a comunicação como ferramentas estratégicas para atingir os objetivos organizacionais (ibidem, 2004, p. 651). Em contrapartida, a perspetiva cocreacional encara os públicos como cocriadores de significado e comunicação, possibilitando a compreensão de significados, interpretações e objetivos comuns (ibidem, 2004, p. 652). Esta perspetiva coloca um valor implícito nas relações que vão para além da concretização de um objetivo organizacional, pelo que os públicos se constituem como parceiros no processo de criação de sentido (ibidem, 2004, p. 652). No fundo, os autores acreditam que:

> *Ao longo dos últimos 20 anos, as relações públicas evoluíram para uma importante área de comunicação aplicada baseada na investigação de quantidade e qualidade significativas. As relações públicas tornaram-se muito mais do que uma mera prática de comunicação empresarial. Pelo contrário, é uma área teoricamente fundamentada e baseada na investigação que tem potencial para unificar uma variedade de áreas de comunicação aplicada e servir diferentes tipos de organizações, incluindo organizações sem fins lucrativos com agendas pró-sociais* (Botan & Taylor, 2004, p. 659)

Enquanto parte de um "sistema" organizacional, caracterizado por um conjunto de subsistemas que interagem entre si, as Relações Públicas desempenham um papel "de limite", o que significa que funcionam na fronteira da organização, servindo de ligação entre esta e os seus *stakeholders* – a chamada Teoria Geral dos Sistemas (Grunig & Hunt, 1984, p. 9). Neste sentido, os profissionais de Relações Públicas apoiam outros subsistemas da organização, ajudando-os a comunicar não só através dos limites da organização com o público externo, mas também com outros subsistemas internos à organização (ibidem, 1984, p. 9).

A relação entre a organização, os seus públicos e o subsistema de gestão organizacional pode ser sintetizada através do modelo apresentado na Figura 1 (Grunig & Hunt, 1984, p. 10).

Figura 1: Modelo da função de Relações Públicas numa organização (adaptado de Grunig & Hunt, 1974)



O conjunto de setas na base do triângulo da Figura 1 indica que as organizações e os públicos têm consequências recíprocas entre si, o que significa que as decisões tomadas pelo subsistema de gestão de uma organização podem ter consequências sobre o público, da mesma forma que o público, muitas vezes, toma medidas que têm consequências para a organização (Grunig & Hunt, 1984, p. 10). Para mediar esta relação entre a organização e os públicos, destaca-se então o papel fundamental das Relações Públicas que, através da comunicação, procuram obter informação de ambas as partes relativamente aos comportamentos e atitudes da outra parte e, assim, garantir que são tomadas decisões orientadas em função dos interesses de todas as partes (ibidem, 1984, p. 11).

1.3. Os quatro modelos pioneiros na área das Relações Públicas

O contributo de Grunig e Hunt (1984) foi especialmente importante na história das Relações Públicas, ao institucionalizar os quatro modelos de Relações Públicas, percecionados como o verdadeiro "motor de arranque" para a discussão académica em torno da área (Gonçalves, 2010, p. 25). Os autores entenderam os modelos da seguinte forma:

- *Press Agentry/Publicity*: as Relações Públicas servem uma função de propaganda, cujo principal objetivo é difundir a cultura da organização, muitas vezes através de informação incompleta, distorcida ou meia-verdade;
- *Public Information*: o objetivo é a divulgação de informação sobre a organização, não necessariamente com uma intenção persuasiva;
- *Two-Way Asymmetric*: as Relações Públicas assumem um propósito de persuasão científica, procurando persuadir as atitudes e comportamentos do público face à organização;

- *Two-Way Symmetric*: o objetivo é a compreensão mútua entre as organizações e os seus públicos (Grunig & Hunt, 1984, pp. 21-22).

Ao nível da natureza da comunicação, os dois primeiros modelos privilegiam a comunicação unidirecional, desde a organização até ao público, muito embora difiram em termos da informação transmitida – no modelo *press agentry/publicity* nem sempre é apresentada uma imagem completa da organização, contrariamente ao que se sucede no modelo *public information* (Grunig & Hunt, 1984, p. 23). Os outros dois modelos caracterizam-se pela comunicação bidirecional entre a organização e os seus públicos (ibidem, 1984, p. 23). Todavia, a grande diferença é que no modelo *two-way asymmetric* os efeitos das Relações Públicas são desequilibrados a favor da organização, assistindo-se a uma vontade de tentar mudar unicamente as atitudes e comportamentos do público, enquanto o modelo *two-way symmetric* consiste mais num diálogo, em que ambas as partes – organização e públicos – têm a mesma probabilidade de persuadir as atitudes e comportamentos da outra parte (ibidem, 1984, p. 23).

Considerado como o modelo normativo das Relações Públicas, tanto numa perspetiva histórica como teórica (Gonçalves, 2010, p. 29), o modelo *two-way symmetric* descreve um nível de igualdade de comunicação pouco frequentemente encontrado na vida real, em que cada parte está disposta a alterar o seu comportamento para acomodar as necessidades da outra, resultando em relações de poder equilibradas (Theaker, 2012, p. 36). Como resultado, a comunicação bidirecional simétrica produz melhores relações a longo prazo com os públicos comparativamente aos restantes modelos de Relações Públicas (Grunig *et al.*, 2002, p. 15). Significativamente, parece ser utilizado mais por organizações sem fins lucrativos, agências governamentais e organismos regulados e não tanto por empresas competitivas e orientadas para o lucro (Butterick, 2011, p. 28).

1.4. As diferentes perspetivas e paradigmas acerca da prática de Relações Públicas

Em 2011, Grunig debruçou a sua atenção sobre os paradigmas que considera estarem na base da prática das Relações Públicas: o paradigma simbólico-interpretativo e o paradigma comportamental (p. 13). O paradigma simbólico-interpretativo pressupõe que as Relações Públicas se esforçam por influenciar a forma como os públicos interpretam os comportamentos das organizações, assim como assegurar o poder dos decisores que escolhem esses comportamentos (ibidem, 2011, p. 13). Já o paradigma comportamental ou de gestão estratégica centra-se na participação dos executivos de Relações Públicas na tomada de decisões estratégicas, com o intuito de ajudar a gerir o comportamento das organizações, em vez de apenas o interpretarem para o público (ibidem, 2011, p. 13).

Com o intuito de desmitificar a função puramente interpretativa da atividade, Grunig (2011) formula a sua própria perspetiva acerca do papel estratégico das Relações Públicas, acreditando que as Relações Públicas proporcionam às organizações uma forma de dar voz e poder ao público na tomada de decisões organizacionais – uma perspetiva pós-moderna – e, simultaneamente, beneficiam as organizações ao ajudá-las a tomar decisões, desenvolver políticas, prestar serviços e comportar-se de formas que sejam aceites e desejadas pelo público – uma perspetiva semi-modernista (p. 15). Perante a necessidade de estabelecer a forma como os profissionais de Relações Públicas devem participar na gestão estratégica de uma organização, é desenvolvido o modelo de gestão estratégica das Relações Públicas, sustentado na interligação dos conceitos centrais de decisões de gestão de topo, *stakeholders* e públicos, bem como nos resultados destas relações (ibidem, 2011, p. 17). O modelo pressupõe que os decisores estratégicos de uma organização devem interagir com os *stakeholders* através da função de Relações Públicas, não só porque as suas decisões têm consequências para o público, mas também porque a organização necessita de relações de apoio com os *stakeholders* para tomar decisões responsáveis, implementar ações e atingir objetivos organizacionais (ibidem, 2011, p. 17).

A verdade é que as Relações Públicas podem ser definidas tendo por base duas perspetivas – académica e profissional –, que partilham os mesmos conceitos-chave: relações (trocas); comunicação (tornar comum); processo e continuidade; intencionalidade; planeamento; organização; e públicos (grupos) (Sebastião, 2012, p. 26). Segundo a autora:

> *As relações públicas não são intuição ou imagem; são uma atividade profissional cujos mérito e reconhecimento têm crescido nos últimos anos, graças à configuração globalizante da economia, do sistema capitalista informacional, ao desenvolvimento das tecnologias da informação e da comunicação e à tomada de consciência do papel da comunicação e da troca/embate de interesses e de influência nas organizações contemporâneas* (Sebastião, 2012, p. 39)

Contudo, Sebastião (2012) defende que as Relações Públicas só podem ser exercidas na base de uma filosofia profissional, ética e socialmente responsável (p. 27). Em termos do seu carácter ético e moral, as Relações Públicas devem assentar numa postura de respeito pelo homem e pelas regras da boa fé e do bom senso, por forma a conferir credibilidade à profissão e ao próprio setor (ibidem, 2012, pp. 39-40). Do ponto de vista social, devem igualmente promover o diálogo social, humanizar a face do Estado e defender os direitos de liberdade e igualdade dos cidadãos (ibidem, 2012, p. 40). Enquanto função organizacional, devem assumir uma comunicação

bidirecional, rejeitando a manipulação dos públicos e da opinião pública por parte dos líderes organizacionais (ibidem, 2012, p. 40).

Por sua vez, Eiró-Gomes e Nunes (2013) vão mais além e sugerem uma reformulação do conceito de Relações Públicas, adaptado à realidade da sociedade contemporânea:

> *Cada vez mais é urgente que as organizações, os governos, os Estados, consigam o goodwill dos seus públicos, a sua confiança e compromisso. Cada vez mais é necessário que, acima do próprio interesse da "organização" haja um interesse comum que beneficie a sociedade como um todo. Estaremos, aqui, perante um novo paradigma das Relações Públicas, uma nova definição desta atividade, adaptada às exigências das sociedades modernas e futuras* (Eiró-Gomes & Nunes, 2013, p. 1056)

Brom e Sha (2013) partilham da mesma opinião, ao afirmar que os profissionais de Relações Públicas que ajudam as organizações a estabelecer e manter relações mutuamente benéficas desempenham uma função essencial de gestão que tem impacto na sociedade em geral, no sentido em que encorajam a responsabilidade social nas organizações e promovem o papel essencial das Relações Públicas na manutenção da ordem social (p. 78).

De forma resumida, Wilcox *et al.* (2012) sugerem um conjunto de palavras-chave que permitem definir o conceito de Relações Públicas, sendo elas (p. 7):

- Deliberação: a atividade de Relações Públicas é intencional, sendo concebida para influenciar, ganhar compreensão, fornecer informação e receber *feedback*;
- Planeamento: a atividade de Relações Públicas é organizada e sistemática, exigindo investigação e análise;
- Resultados: as Relações Públicas eficazes baseiam-se em políticas e resultados reais;
- Interesse público: a atividade de Relações Públicas deve ser mutuamente benéfica, procurando alinhar os interesses da organização com os interesses e preocupações dos seus públicos;
- Comunicação bilateral: a atividade de Relações Públicas é mais do que a divulgação de informação num único sentido, revelando-se necessário solicitar e obter *feedback*;
- Função de gestão: a atividade de Relações Públicas é mais eficaz quando se constitui como parte integrante do processo de tomada de decisões organizacionais, devendo fornecer aconselhamento e resolução de problemas ao mais alto nível.

Contrariamente à maioria das abordagens de Relações Públicas, Ihlen e van Ruler (2007) defendem uma visão orientada para a sociologia, que se centra na relação que a atividade de Relações Públicas tem com a sociedade em que é produzida e com os sistemas sociais que co-produz (p. 244). Neste caso, à semelhança da maioria das abordagens sociológicas, as Relações Públicas estão relacionadas com a questão empírica do que é bom e justificável para os membros da sociedade (ibidem, 2007, p. 245).

O atual paradigma dominante em Relações Públicas é a Teoria da Excelência, que procura compreender de que forma as Relações Públicas, enquanto função de gestão, contribuem para a eficácia organizacional (Grunig *et al.*, 2002, p. 10). Estando ciente de que a construção de relações com os públicos é a essência das Relações Públicas, compreende-se que a qualidade das relações com públicos estratégicos se constitui como um indicador-chave da contribuição a longo prazo que as Relações Públicas conferem à eficácia organizacional (ibidem, 2002, pp. 10-11). De acordo com esta visão, as Relações Públicas devem servir os interesses tanto da organização como da sociedade, conciliando os objetivos estratégicos com as expectativas dos públicos (ibidem, 2002, p. 97). Tal como afirma Butterick (2011), esta teoria defende que a forma mais eficaz de comunicação, tanto externa como internamente, centra-se numa abordagem simétrica, o que significa que as organizações devem não só empenhar-se numa comunicação construtiva bilateral com os seus públicos, como também devem estar preparadas para mudar a sua política como resultado desse diálogo (p. 32).

De acordo com um estudo levado a cabo por Tam *et al.* (2020), compreendeu-se que uma função de Relações Públicas com poder (ou seja, sendo uma função de delimitação entre a gestão e os públicos estratégicos) confere uma maior capacidade de absorção organizacional no aproveitamento de oportunidades, assim como uma diminuição da incerteza ambiental (p. 6). Isto significa que uma função de Relações Públicas fortalecida reflete tanto um ambiente empresarial participativo como esforços de investigação estrategicamente orientados, o que, por sua vez, cria uma organização anfitriã estrategicamente orientada (ibidem, 2020, p. 18). A verdade é que os esforços de investigação dos gestores de Relações Públicas e a cultura organizacional participativa têm efeitos notáveis no empoderamento das Relações Públicas devido à maior perceção da criação de valor das Relações Públicas por parte dos gestores de topo (ibidem, 2020, p. 18).

Tendo por base a premissa da comunicação em Relações Públicas, Kent e Taylor (2002) definem os seguintes pressupostos como orientação do diálogo entre a organização e os seus públicos (pp. 24-25):

- Mutualidade: o reconhecimento das relações organização-público;
- Propensão: a temporalidade e espontaneidade das interações com o público;
- Empatia: o apoio e confirmação dos objetivos e interesses do público;
- Risco: a vontade de interagir com indivíduos e públicos nos seus próprios termos;
- Compromisso: medida em que uma organização se entrega ao diálogo, à interpretação e compreensão nas suas interações com o público.

Para que qualquer abordagem ao diálogo seja eficaz, revela-se necessário um compromisso organizacional e uma aceitação do valor da construção de relações, existindo três formas de incorporá-lo na prática das Relações Públicas (Kent & Taylor, 2002, pp. 30-32):

- Diálogo interpessoal: os líderes organizacionais – e eventualmente todos os membros da organização que comunicam com o público – devem sentir-se confortáveis no diálogo e, como tal, deter um conjunto de competências, como saber ouvir, ser empático, pensar em objetivos a longo prazo ou solicitar uma variedade de opiniões internas e externas;
- Diálogo mediado: as organizações podem reforçar o seu empenho no diálogo e fomentar uma maior interação com o público, utilizando canais mediados de massa para comunicar com o público;
- Diálogo organizacional/ processual: esta abordagem envolve a criação de mecanismos organizacionais para facilitar o diálogo.

2. A reputação enquanto ativo fundamental para o sucesso organizacional

2.1. Reputação organizacional: a institucionalização do conceito

A partir dos anos 50, o conceito de reputação começou a ganhar relevância na literatura académica (Berens & van Riel, 2004, p. 161). Não obstante, a reputação constitui-se como um fenómeno complexo, que merece a devida atenção e, por conseguinte, uma gestão adequada (Davies & Miles, 1998, p. 16).

A complexidade na definição da reputação pode ser justificada pelo facto de existirem duas visões sobre o conceito que se apresentam de forma distinta: a perspetiva económica e a perspetiva narrativa (Jorge, 2011, p. 3264). Por um lado, a perspetiva económica defende o valor da reputação e posiciona-a enquanto ativo intangível de uma organização, sendo valorizada pelo mercado e contribuindo diretamente para o sucesso organizacional (ibidem, 2011, p. 3265). Esta perspetiva fundamenta-se na definição base proposta por Fombrun e van Riel (1997), considerada unificada e transversal às diferentes disciplinas que abordam o tema:

> *A reputação corporativa é uma representação coletiva das ações e resultados passados de uma organização, que descreve a sua capacidade em criar valor para os seus múltiplos stakeholders. Avalia a posição relativa de uma organização a nível interno, através dos seus colaboradores, e a nível externo, através dos seus stakeholders, tanto no seu ambiente competitivo como institucional* (Fombrun & van Riel, 1997, p. 10)

Mais tarde, acrescentaram à sua definição que as reputações se constituem como perceções agregadas pelos *stakeholders* relativamente à capacidade de uma organização para satisfazer as suas expectativas, quer estejam interessados em adquirir os produtos ou serviços da organização, trabalhar para a organização ou investir nas suas ações (van Riel & Fombrun, 2007, p. 43).

Não obstante, Jorge (2011) sublinha que, apesar do importante contributo da perspetiva económica para a construção do conceito de reputação, a natureza complexa das relações entre a organização e os seus *stakeholders* não pode ser exclusivamente entendida com base no discurso financeiro (p. 3268). É neste sentido que a perspetiva narrativa assume igual destaque ao defender que a reputação é subjetiva e construída socialmente, tendo por base a atribuição de significados por parte dos *stakeholders*, que partilham entre si emoções, atitudes e histórias da organização (ibidem, 2011, p. 3268). Para o autor, a reputação deve ser interpretada como uma interligação destas duas perspetivas: o poder da reputação é construído a partir dos significados que surgem através da noção de sentido narrativo que é a história da organização, criando uma expectativa que influencia o comportamento dos *stakeholders* perante a organização, valorizando-a e aumentando o seu valor intangível (ibidem, 2011, p. 3270).

Por sua vez, Gotsi e Wilson (2001) acreditam que a reputação consiste numa avaliação global da organização ao longo do tempo, baseando-se nas experiências diretas dos *stakeholders* com a organização, qualquer outra forma de comunicação e simbolismo que forneça informações sobre as ações da organização e/ou uma comparação com as ações dos principais concorrentes (p. 29). Já Barnet *et al.* (2006) defendem que esta avaliação é criada pelos *stakeholders* em função dos impactos financeiros, sociais e ambientais atribuídos à organização ao longo do tempo (p. 34).

Segundo Weigelt e Camerer (1988), uma reputação corporativa é um conjunto de atributos associados a uma organização, inferidos a partir das suas ações passadas (p. 443). Tal como sublinham Barnett e Hoffman (2008), ao determinar a reputação de uma organização, os *stakeholders* fazem julgamentos sobre os comportamentos passados de uma organização e desenvolvem, por conseguinte, expectativas sobre os seus comportamentos futuros (p. 4). Pode-se, portanto, depreender que uma reputação funciona como um instrumento que permite aos *stakeholders* prever com maior precisão os comportamentos de uma organização (ibidem, 2008,

p. 4). Mahon (2002) denomina este fenómeno de "expectativas reputacionais", argumentando que a organização tem de considerar as suas ações anteriores e a gestão da sua reputação ao reagir a uma nova situação (p. 424).

Sob uma perspetiva diferente, Schwaiger (2004) entende a reputação como uma construção de atitude que implica a combinação de componentes afetivos e cognitivos, em que a atitude denota uma mentalidade subjetiva, emocional e cognitiva (p. 49). Significa isto que a reputação corporativa não só avalia as perceções subjetivas dos atributos de uma organização – tais como "empresa de sucesso" ou "produtos de alta qualidade" –, mas também permite uma disposição intrínseca em relação a estes atributos (ibidem, 2004, p. 49). Dado que a reputação corporativa se baseia muito mais em perceções do que em conhecimentos reais, a gestão da reputação corporativa é, sobretudo, uma tarefa de comunicação corporativa (ibidem, 2004, p. 67).

2.2. O valor da reputação no seio das organizações

A verdade é que as organizações bem-sucedidas reconhecem a reputação como um instrumento de diferenciação entre as organizações (Dolphin, 2004, p. 84). Por esse motivo, os executivos de comunicação percecionam a gestão da reputação como forma de gestão de ativos, constituindo-se como um elemento central da sua estratégia de comunicação e detendo um papel fundamental na governação empresarial (ibidem, 2004, pp. 87-88). Neste sentido, pode-se entender a reputação como um ativo intangível que é escasso, valioso, sustentável e difícil de imitar por uma organização concorrente, pelo que se constitui como um instrumento adequado para alcançar vantagens competitivas estratégicas (Schwaiger, 2004, p. 51).

É inegável o valor da reputação para as organizações (Lewis, 2001, p. 31). Segundo Roberts e Dowling (2002), os ativos intangíveis – como as boas reputações – são críticos devido ao seu potencial de criação de valor, mas também porque o seu carácter intangível torna a replicação por empresas concorrentes consideravelmente mais difícil (p. 1077). Não obstante, uma boa reputação é um ativo valioso que permite a uma organização alcançar, acima de tudo, uma rentabilidade persistente ou um desempenho financeiro superior sustentado (ibidem, 2002, p. 1078). Schnietz e Epstein (2005) defendem, inclusive, que uma boa reputação protege uma organização de perdas financeiras durante uma crise (p. 341).

A reputação de uma organização pode não depender unicamente das suas ações, mas também das ações das organizações concorrentes, que acabam por moldar a reputação organizacional e, em última análise, o seu desempenho (Barnett & Hoffman, 2008, p. 1). Posto isto, o mau comportamento de uma organização pode prejudicar a reputação de todas as

organizações da indústria, da mesma forma que o comportamento exemplar de uma organização pode aumentar as expectativas, levando a um declínio na reputação das organizações que não acompanham o ritmo (ibidem, 2008, p. 2). Para gerir eficazmente a reputação corporativa, as organizações precisam de compreender não só de que forma as suas reputações e o seu desempenho são influenciados pela interdependência interorganizacional, assim como de que forma podem gerir esta interdependência (ibidem, 2008, p. 2).

Contrariando a ideia de que a reputação é vantajosa somente para a organização, Fombrun e Shanley (1990) sublinham que as próprias reputações estabelecidas funcionam como sinais que também influenciam as ações dos *stakeholders* (p. 234). Tal como afirma Chun (2005), a reputação afeta a forma como os diversos *stakeholders* se comportam em relação à organização, influenciando, por exemplo, a retenção de colaboradores, a satisfação do cliente e a sua lealdade perante a organização (p. 91). Significa isto que a reputação influencia as relações da organização com os seus *stakeholders* (Lange *et al.*, 2011, p. 154).

Por sua vez, Mendes (2013) sugere que a reputação apresenta algumas componentes fundamentais:

> *É uma estimativa/avaliação das ações que as organizações tiveram (feita interna ou externamente à organização), mas ao mesmo tempo, uma expectativa sobre comportamentos futuros, demonstrando o seu desenvolvimento dinâmico ao longo do tempo. Tem a ver, por isso, com notoriedade, admiração, caráter, valores e ética; no fundo, com o reconhecimento daquilo que a organização é e com o impacto que produz naqueles com que ela se relaciona, permitindo distinção e vantagens comparativa e competitiva, nos mercados e sociedades em que atua* (Mendes, 2013, p. 30)

Analisando o seu processo de formação, é possível afirmar que uma reputação se forma a partir de redes de associações cognitivas que se desenvolvem ao longo do tempo a partir da exposição cumulativa de um grupo a estímulos sensoriais, construindo, assim, uma impressão global da organização (van Riel & Fombrun, 2007, p. 46). Acredita-se que a maior influência na reputação acontece ao nível primário, a partir da experiência pessoal direta, embora a maior parte da informação seja adquirida indiretamente de amigos e através do poder amplificador dos *media* (ibidem, 2007, p. 46). Assim, quanto mais os *stakeholders* confiam na reputação de uma organização para tomar decisões de compra ou investimento, mais importante é que a organização tenha uma reputação forte (ibidem, 2007, p. 47).

Todavia, a perceção da reputação por parte dos *stakeholders* pode também ser moldada, em certa medida, pelas ações deliberadas da organização que estão a avaliar, com o intuito de influenciar a criação de uma perceção favorável em relação à mesma (Davies *et al.*, 2003, p. 74). A organização pode gerir a perceção da sua reputação através daquilo que optar por comunicar aos seus *stakeholders* (ibidem, 2003, p. 74).

2.3. Os conceitos de identidade e imagem no processo de construção da reputação organizacional

A partir da década de 90, termos como identidade, imagem, prestígio, *goodwill*, estima e estatuto foram utilizados como sinónimos ou em relação muito próxima com o conceito de reputação (Wartick, 2002, p. 373). Barnett *et al.* (2006) acreditam, inclusive, que a principal barreira para a criação de uma definição consensual acerca do conceito de reputação esteja relacionada com a confusão entre os conceitos de identidade, imagem e reputação (p. 28).

No sentido de melhor compreender esta relação entre conceitos, importa refletir acerca dos conceitos de identidade e imagem de forma isolada.

- **Identidade corporativa**

Por um lado, a identidade corporativa é fundamentada no mote "Como nos vemos a nós próprios", ou seja, como os colaboradores se entendem a si próprios em relação à cultura e aos valores organizacionais (Chun, 2005, p. 97). Tal como afirma Fombrun (1996/2018), a identidade corporativa descreve o conjunto de valores e princípios que os colaboradores associam a uma organização (p. 99). Quer seja amplamente partilhada ou não, uma identidade corporativa reúne as características geralmente compreendidas pelos colaboradores relativamente ao trabalho efetuado, produtos comercializados e relação com os clientes e os investidores de uma organização (ibidem, 2018, p. 99).

Percecionada como a realidade e singularidade de uma organização, a identidade corporativa pode ser gerida através da interação dinâmica entre a estratégia empresarial da empresa, a filosofia dos seus principais executivos, a sua cultura corporativa e o seu desenho organizacional (Gray & Balmer, 1998, p. 695). Adicionalmente, a identidade corporativa pode ser conceptualizada como uma coleção de símbolos (Barnett *et al.*, 2006, p. 34).

- **Imagem corporativa**

No que se refere à imagem corporativa, Gray e Balmer (1998) entendem-na como a imagem mental da organização detida pelo seu público, ou seja, o que nos vem à mente quando vemos e ouvimos o nome da organização ou quando vemos o seu logótipo (p. 696), correspondendo ao mote "Como os outros nos veem" (Chun, 2005, p. 95).

O processo de transição da identidade para a imagem é essencialmente uma função de Relações Públicas que tenta moldar a impressão que as pessoas têm da organização (Barnett *et al.*, 2006, p. 34). Contudo, Fombrun (1996/2018) acredita que a imagem corporativa nem sempre reflete com exatidão a identidade da organização; na maioria das vezes, a imagem é distorcida não só quando a organização tenta manipular o seu público através da publicidade ou outras formas de auto-apresentação, mas também quando se desenvolvem rumores tendo por base declarações não oficiais por parte de alguns *stakeholders* (p. 100).

Quando comparada com a reputação, a imagem corporativa pode ser criada mais rápida e facilmente (Gray & Balmer, 1998, p. 696). Uma imagem forte pode ser construída através de uma campanha coordenada de construção de imagem que engloba um sistema de comunicação formal – nome, logótipo, sinalética, publicidade corporativa e Relações Públicas (ibidem, 1998, p. 696). Em contrapartida, uma reputação favorável requer, além de um esforço de comunicação eficaz, uma identidade meritória que só pode ser moldada através de um desempenho consistente, geralmente ao longo de muitos anos (ibidem, 1998, p. 696). Além disso, a reputação pode não estar aberta à manipulação, enquanto a imagem pode ser claramente manipulada (Dolphin, 2004, p. 89). No entanto, numa situação de crise, tanto a imagem como a reputação podem ser danificadas muito rapidamente (Chun, 2005, p. 96).

De forma resumida, Wartick (2002) refere que a identidade deve ser uma construção centrada nos *stakeholders* internos; a imagem deve estar principalmente relacionada com os clientes e com os restantes *stakeholders* externos; e a reputação torna-se, então, a agregação da imagem e da identidade (p. 376). É neste sentido que Davies *et al.* (2003) propõem o modelo da cadeia de reputação corporativa, fundamentado na ideia de que a identidade influencia a imagem, ou seja, a perceção dos colaboradores da organização influencia a visão dos agentes externos, resultando na construção da reputação corporativa (p. 75).

3. A importância da comunicação no processo de gestão de crise

3.1. Crise: um conceito interpretado à luz da perceção dos *stakeholders*

Embora a gestão de crises seja largamente estudada pelos investigadores, Coombs (2007/2019) sublinha a ausência de uma definição consensualmente aceite para o conceito de crise (p. 18). Não obstante, na tentativa de oferecer uma síntese de várias perspetivas de crise apresentadas por outros autores, Coombs (1999/2019) propõe a seguinte definição:

> *Uma crise é a perceção de violação das expectativas dos stakeholders, que pode resultar em consequências negativas para os stakeholders e/ou para a organização* (Coombs, 1999/2019, p. 19)

A interpretação de um evento enquanto crise varia consoante a perceção que cada *stakeholder* tem acerca da situação, o que significa que uma crise apenas existe se os *stakeholders* reagirem à organização como se ela estivesse em crise (Coombs, 1999/2019, p. 19). Acrescenta-se que uma crise é um acontecimento repentino e inesperado que ameaça perturbar o normal funcionamento de uma organização, representando tanto uma ameaça financeira como uma ameaça reputacional (Coombs, 2007, p. 164). As crises podem prejudicar os *stakeholders* quer a nível físico, emocional ou financeiro (ibidem, 2007, p. 164).

Pearson e Clair (1998) defendem que uma crise organizacional é uma situação de baixa probabilidade, de alto impacto, que é percecionada como uma ameaça à visibilidade da organização e que é subjetivamente vivida pelos *stakeholders* como pessoal e socialmente ameaçadora (p. 66). Devido ao seu carácter altamente saliente, inesperado e potencialmente perturbador, uma crise pode ameaçar os objetivos de uma organização e ter profundas implicações nas suas relações com os *stakeholders* (Bundy *et al.*, 2016, p. 2). Coombs e Holladay (2010) acrescentam que uma crise pode também colocar exigências não rotineiras sobre uma organização, gerar incerteza, ter um impacto negativo no desempenho organizacional e produzir resultados negativos para a organização (p. 97).

A verdade é que as crises se constituem como uma ameaça à reputação, pelo que a resposta comunicativa de uma organização a uma crise pode servir para limitar e até para reparar os danos à reputação (Coombs & Holladay, 2002, p. 166). Se as organizações não responderem adequadamente às crises, a sua reputação muito provavelmente sairá prejudicada (Ma & Zhan, 2016, p. 1).

3.2. A necessidade de comunicação de crise para uma eficaz gestão de crise

É neste sentido que a gestão de crises assume um papel fundamental. Segundo Pearson e Mitroff (1993), o objetivo da gestão de crises passa por preparar uma organização para pensar criativamente sobre o impensável, de modo que as melhores decisões sejam tomadas em tempo de crise (p. 59). A gestão de crises exige que sejam tomadas medidas estratégicas tanto para evitar ou mitigar desenvolvimentos indesejáveis, como para proporcionar uma solução desejável para os problemas, devendo ser, portanto, um esforço contínuo por parte da organização (Burnett, 1998, p. 476). Para ser eficaz e beneficiar as organizações, a gestão de crises deve procurar proteger e ajudar, sobretudo, os *stakeholders* colocados em risco em situação de crise (Coombs & Holladay, 2010, p. 23).

Para Coombs (1999/2019), a gestão de crises procura prevenir ou atenuar os resultados negativos de uma crise e, assim, proteger a organização e os *stakeholders* de eventuais danos, compreendendo um conjunto de quatro fatores: a) prevenção – representa as medidas tomadas para evitar a ocorrência de crises; b) preparação – pretende preparar a organização para enfrentar uma eventual crise; c) resposta – consiste na aplicação dos componentes de preparação para uma crise; d) avaliação – corresponde à avaliação da resposta da organização em situação de crise, considerando os esforços de prevenção, preparação e resposta da organização em futuras situações de crise (pp. 21-22).

Enquanto componente crítica da gestão de crises, a comunicação de crise pode ser definida como a recolha, processamento e divulgação da informação necessária para enfrentar uma situação de crise (Coombs & Holladay, 2010, p. 20). Antes da ocorrência da crise, a comunicação centra-se na recolha de informação sobre riscos de crise, tomada de decisões sobre como gerir eventuais crises e formação de pessoas que estarão envolvidas no processo de gestão de crise (ibidem, 2010, p. 20). Após a ocorrência da crise, a comunicação envolve a dissecação do esforço de gestão de crise, a transmissão das mudanças necessárias e o fornecimento de mensagens de acompanhamento da crise (ibidem, 2010, p. 20).

A gestão da comunicação de crise centra-se em comunicar com os *stakeholders* afetados durante o rescaldo de uma crise e continuar através do período de turbulência gerado pela crise (Sturges, 1994, p. 297). Para além de lidar com as consequências da crise, o objetivo da comunicação de crise passa por influenciar o desenvolvimento da opinião pública de tal forma que as opiniões mantidas no período pós-crise sejam maioritariamente positivas, ou pelo menos se mantenham ao mesmo nível do período pré-crise (ibidem, 1994, p. 303). Por esse motivo, à medida que uma crise avança ao longo do seu ciclo de vida, a gestão deve preocupar-se com três categorias

de informação: a) informação de instrução – como devem as pessoas reagir fisicamente à crise; b) informação de ajustamento – ajuda as pessoas a lidar psicologicamente com a crise; e c) informação de internalização – é utilizada pelas pessoas para formular uma imagem positiva da organização (ibidem, 1994, p. 308).

Revela-se, portanto, necessário diferenciar dois tipos básicos de comunicação de crise: a) a gestão do conhecimento de crises, que envolve a identificação de fontes, a recolha de informação, a análise de informação, a partilha de conhecimento e a tomada de decisões; e b) a gestão de reações dos *stakeholders*, que compreende esforços comunicativos para influenciar a perceção dos *stakeholders* sobre a crise, sobre a organização em crise e sobre a resposta da organização à crise (Coombs & Holladay, 2010, p. 25).

Numa tentativa de esclarecer de que forma podem as organizações responder eficazmente às crises, González-Herrero e Pratt (1996) sugerem um modelo que integra quatro etapas simétricas: a) gestão de questões – a organização deve analisar o ambiente e identificar questões problemáticas que a possam afetar futuramente, com o intuito de desenvolver uma estratégia de comunicação centrada na prevenção de ocorrência de uma crise; b) planeamento/ prevenção – a organização deve desenvolver um plano de contingência para mitigar uma eventual crise; c) crise – a organização deve reagir prontamente aos acontecimentos e utilizar medidas de contingência que possam reduzir quaisquer danos causados pelo incidente; e d) pós-crise – a organização deve continuar a acompanhar a situação, procurando manter os seus *stakeholders* informados e desenvolvendo programas de comunicação a longo prazo para reduzir os danos causados pela crise (pp. 89-100).

Tendo por base o estudo desenvolvido por Pearson e Mitroff (1993), foi possível concluir que existem quatro variáveis principais que influenciam a gestão de crises, sendo elas: a) tipos de crise – a preparação para uma crise organizacional começa com uma compreensão da natureza específica da crise; b) fases da crise – a crise inicia-se com um conjunto de sinais de alerta precoce, levando a organização a prevenir uma eventual situação de crise, passando pela contenção de danos e posterior recuperação do negócio, o que culmina numa aprendizagem organizacional; c) sistemas da crise – a crise pode ocorrer em diferentes sistemas, nomeadamente técnico, humano, infraestrutural, cultural e emocional; e d) intervenientes da crise – a crise pode ser provocada pela grande variedade de *stakeholders* da organização (pp. 49-56).

Por sua vez, Burnett (1998) argumenta que o processo de gestão de crises reúne cinco componentes básicos, nomeadamente: a) um conjunto de condições antecedentes

(internas/externas) que determinam o grau de controlo da organização sobre o seu ambiente, bem como a sua suscetibilidade à crise; b) uma tipologia de crises – baseada na suscetibilidade, controlo, consequências negativas ou positivas, e semelhanças estruturais – que se constitui como o sistema inicial de deteção de crises; c) um mecanismo de avaliação de crises que considera o nível de ameaça relativa, restrições de tempo, os decisores envolvidos, a quantidade e qualidade da informação e as implicações das decisões tomadas a curto e longo prazo; d) o estabelecimento de uma estrutura organizacional para a gestão de crises que sugere um padrão de resposta a nível individual e organizacional; e e) um mecanismo para avaliar o sucesso das soluções (p. 479).

Por conseguinte, Burnett (1998) enumera um conjunto de características que parecem comuns a todas as crises: a) as crises são determinadas por perceções individuais e não por factos objetivos; b) as crises são frequentemente resolvidas durante um curto período de tempo; c) as crises são difíceis de gerir devido ao controlo limitado sobre o ambiente; e d) quando ocorrem numa parte da organização, as crises têm implicações para todos os restantes elementos organizacionais (p. 479).

Estando ciente de que as crises são indesejáveis e súbitas (González-Herrero & Pratt, 1996, p. 82), Coombs (1999/2019) reforça que todas as organizações devem preparar-se para lidar com as crises, tomando seis medidas: a) diagnóstico de vulnerabilidades; b) avaliação dos tipos de crise; c) seleção e formação de uma equipa de gestão de crise; d) seleção e formação de um porta-voz; e) desenvolvimento de um plano de comunicação de crise; e f) revisão do sistema de comunicação de crise (p. 58).

3.3. As diferentes fases de gestão de uma crise

Posto isto, o conjunto de fatores que constituem a gestão de crises pode ser dividido em três categorias: pré-crise, crise e pós-crise (Coombs & Holladay, 2010, p. 20). Estas três categorias refletem as diferentes fases da gestão de crises, sendo úteis por fornecer um mecanismo para considerar a amplitude da comunicação de crises (ibidem, 2010, p. 20).

3.3.1. Fase pré-crise

Nesta fase, a comunicação de crise concentra-se na localização e redução do risco, por forma a prevenir a ocorrência de uma eventual crise (Coombs & Holladay, 2010, p. 25). De acordo com Coombs (1999/2019), esta fase envolve três sub-etapas (p. 25):

- Deteção de sinais: os gestores de crise devem identificar fontes de sinais de aviso, recolher informação relacionada com os mesmos e analisar a informação;

- Prevenção: uma vez identificada uma potencial crise, devem ser tomadas medidas preventivas, as quais se enquadram em três categorias: a) gestão de questões – significa tomar medidas para evitar que um problema se transforme numa crise; b) gestão de riscos – elimina ou reduz os níveis de risco; e c) gestão da reputação – procura resolver problemas na relação entre a organização e os seus *stakeholders* que possam escalar e prejudicar a reputação corporativa;
- Preparação para a crise: envolve a identificação de vulnerabilidades de crise, a criação de equipas de crise, a seleção de porta-vozes, a elaboração de planos de comunicação de crise, o desenvolvimento de carteiras de crise (uma lista das crises com maior probabilidade de ocorrer) e a estruturação do sistema de comunicação de crise.

No decorrer desta fase, Bundy *et al.* (2016) defendem que, ao nível da perspetiva interna, a organização deve orientar-se – através de mudanças na sua cultura, *design* e estrutura – para evitar quebras de sistema que possam conduzir à ocorrência de crises (p. 7). Em termos da perspetiva externa, a organização deve fomentar relações positivas com os seus *stakeholders*, uma vez que relações negativas podem causar ou agravar situações de crise (ibidem, 2016, p. 9). Além disso, as relações positivas também precisam de se basear em expectativas razoáveis e linhas de comunicação aberta, por forma a evitar a tensão associada a objetivos insustentáveis (ibidem, 2016, p. 9).

3.3.2. Fase de crise

Segundo Coombs e Holladay (2010), compreender de que forma uma organização comunica durante uma situação de crise tem um efeito significativo sobre os resultados da crise, incluindo o número de vítimas e a quantidade de danos reputacionais sofridos pela organização (p. 28). Durante esta fase, os gestores de crise devem perceber que a organização está em crise e tomar medidas adequadas, subdividindo-se em duas fases (Coombs, 1999/2019, p. 25):

- Reconhecimento da crise: inclui uma compreensão de como os eventos são rotulados e aceites como crise, bem como a identificação dos meios para recolher informação relacionada com a crise;
- Contenção da crise: centra-se na resposta a crises organizacionais, incluindo a importância e o conteúdo da resposta inicial, a relação da comunicação com a gestão da reputação, os planos de contingência e as preocupações de acompanhamento.

Bundy *et al.* (2016) acreditam que, durante o evento de crise, a liderança interna é crítica para o processo de gestão de crises (p. 11). Ao nível da perspetiva externa, revela-se necessário ter

em consideração a perceção dos *stakeholders*, que poderá ser influenciada, entre outros, pela escolha das estratégias de resposta à crise, pelo tipo de crise ou pelas avaliações positivas da organização (ibidem, 2016, pp. 13-14).

3.3.3. Fase pós-crise

A comunicação pós-crise é fundamental no período de tempo após uma crise ser considerada resolvida, constituindo-se, em grande parte, como uma extensão da comunicação de resposta à crise, juntamente com a aprendizagem da crise por parte da organização (Coombs & Holladay, 2010, p. 45). À medida que uma organização retoma o seu normal funcionamento, os *stakeholders* devem ser atualizados sobre os esforços de continuidade do negócio (ibidem, 2010, p. 45). Da mesma forma, uma crise proporciona uma oportunidade de avaliar as decisões tomadas pela organização, resultando numa aprendizagem organizacional (ibidem, 2010, p. 46).

Segundo Coombs (1999/2019), as ações pós-crise ajudam a preparar melhor a organização para a próxima crise, assegurar que os *stakeholders* ficam com uma impressão positiva dos esforços de gestão de crise da organização e verificar se a crise está realmente terminada (p. 25).

Por sua vez, Bundy *et al.* (2016) sublinham que, em termos da perspetiva interna, a investigação pós-crise revela que a aprendizagem a partir de uma crise é possível, sujeita a condições que podem influenciar os tipos de lições aprendidas e o grau em que as lições são internalizadas (p. 18). Ao nível da perspetiva externa, grande parte da investigação considera as avaliações sociais de uma organização como resultados-chave de uma crise, incluindo avaliações de reputação, legitimidade e confiança da organização (ibidem, 2016, p. 18).

Durante a década de 90, começou a desenvolver-se uma nova perspetiva sobre gestão de crises denominada abordagem simbólica, que pretendia compreender de que forma a comunicação poderia ser utilizada como um recurso simbólico nas tentativas de proteger a imagem da organização (Coombs, 1998, p. 177). Esta abordagem baseia-se em dois pressupostos fundamentais, nomeadamente: a) as crises são ameaças à imagem de uma organização, pelo que as estratégias de comunicação de crise se constituem como os recursos simbólicos que os gestores de crises utilizam para proteger ou reparar a imagem corporativa; b) as características da situação de crise influenciam as escolhas comunicativas do gestor de crises (ibidem, 1998, pp. 177-178). De acordo com a perspetiva simbólica, a melhor forma de proteger a imagem organizacional é modificando as perceções públicas da responsabilidade pela crise ou as impressões da própria organização (Coombs, 1995, p. 453).

3.4. Teorias do impacto da comunicação de crise no comportamento do público

Para melhor compreender os efeitos da comunicação de crise no comportamento do público, importa refletir acerca das perspetivas que sustentam esta relação: a) teoria de atribuição causal; b) teoria situacional de comunicação de crise; e c) teoria de contingência (Coombs & Holladay, 2010, p. 37).

3.4.1. Teoria de atribuição causal

A teoria de atribuição causal constitui-se como uma teoria sócio-psicológica que procura atribuir uma causa para a ocorrência de eventos (Coombs & Holladay, 2010, p. 37). Significa isto que os indivíduos fazem julgamentos sobre as causas dos acontecimentos, sobretudo os acontecimentos inesperados com resultados negativos (Coombs, 2004, p. 267). Ao identificar a causa do acontecimento, os indivíduos atribuem-lhe a responsabilidade pelo sucedido e, por conseguinte, as atribuições de responsabilidade determinam as suas experiências emocionais perante determinado evento (Weiner, 1985, p. 549).

Segundo Weiner (1985), existem três dimensões causais: a) localização – reflete se a causa do evento é interna ou externa face à organização; b) estabilidade – avalia se a causa do evento é muito ou pouco frequente; e c) controlabilidade – define se a causa do evento é ou não controlável (p. 551).

Posto isto, as dimensões causais da teoria de atribuição permitem estabelecer a seguinte matriz de tipologia de crises (Coombs, 1995, p. 455):

Tabela 1: Matriz de tipologia de crises (adaptado de Coombs, 1995)

	Não intencional	**Intencional**
Externo	*Faux pass*	Terrorismo
Interno	Acidente	Transgressão

Ao nível das crises não intencionais, Coombs (1995) distingue uma crise *faux pass* de um acidente. De natureza externa, um *faux pass* começa quando uma organização toma medidas que acredita serem apropriadas, embora um agente externo redefina as ações da organização como inadequadas, manifestando a sua opinião normalmente sob a forma de boicotes ou protestos (ibidem, 1995, p. 455). A responsabilidade social tende a ser o ponto central que conduz a esta insatisfação, sendo um claro exemplo as campanhas publicitárias relacionadas com o tabaco (ibidem, 1995, p. 455). A um nível interno, os acidentes são involuntários e ocorrem no decurso

de operações organizacionais habituais, como sendo defeitos de produtos, lesões de colaboradores ou acidentes industriais (ibidem, 1995, p. 456).

No que se refere às crises intencionais, Coombs (1995) distingue terrorismo de uma transgressão. Por um lado, o terrorismo refere-se a ações intencionais tomadas por agentes externos, concebidas para prejudicar a organização diretamente – por exemplo, prejudicar colaboradores ou clientes – ou indiretamente – por exemplo, reduzir as vendas ou perturbar a produção (p. 457). Por oposição, a transgressão diz respeito a ações intencionais tomadas por uma organização que, conscientemente, colocam o público em risco, como é o caso de vender produtos defeituosos ou perigosos, ocultar informações de segurança às autoridades, violar leis ou recusar a concessão de recompensas aos clientes (ibidem, 1995, p. 457).

Assim, a responsabilidade por uma crise organizacional deve ser vista como mais forte se a causa for estável (ou seja, a organização tem um historial de crises), se o controlo externo for baixo e se a localização for fortemente interna (ou seja, a intencionalidade é alta) (Coombs & Holladay, 1996, p. 282). Tais atribuições revelam que a organização poderia ter evitado a crise e sabia que poderiam ter sido tomadas medidas preventivas (ibidem, 1996, p. 282). Em contrapartida, a responsabilidade pela crise organizacional deve ser mais fraca quando as atribuições sugerem que a causa é instável (ou seja, a crise é uma exceção na história de desempenho da organização), com um forte controlo externo e uma localização interna fraca (ou seja, a intencionalidade é baixa) (ibidem, 1996, p. 282). Tais condições sugerem que uma organização foi vítima das circunstâncias e que pouco ou nada poderia fazer para prevenir a crise (ibidem, 1996, p. 283).

A teoria da atribuição fornece, portanto, um quadro útil para explicar a relação entre uma situação de crise e a seleção de estratégias de resposta a crises, exploradas pela teoria situacional de comunicação de crise (Coombs, 1995; Coombs, 2004; Coombs, 2007; Coombs & Holladay, 1996).

3.4.2. Teoria situacional de comunicação de crise

A teoria situacional de comunicação de crise assume que a reputação de uma organização é um recurso valioso ameaçado por crises (Coombs & Holladay, 2002, p. 167). Por esse motivo, acredita-se que uma resposta comunicativa estratégica pode ajudar a proteger o recurso de reputação ao selecionar uma estratégia de resposta à crise que se ajuste à situação de crise (ibidem, 2002, p. 167). Tal como defende Coombs (2006), a quantidade de danos à reputação que uma

situação de crise pode infligir impulsiona a seleção das estratégias de resposta à crise por parte da organização (p. 243).

Posto isto, segundo Coombs e Holladay (2010), a teoria situacional de comunicação de crise propõe um processo composto por duas etapas para avaliar a ameaça de crise (p. 39). A etapa inicial consiste em determinar o tipo de crise que a organização enfrenta consoante a responsabilidade que os *stakeholders* lhe conferem (ibidem, 2010, p. 39). Existem, portanto, três tipos de crise, como se pode constatar na Tabela 2: a) vítima – fraca responsabilidade em caso de crise, que se traduz numa ameaça de reputação leve, incluindo desastres naturais, rumores, violência no local de trabalho e violação de produtos; b) acidente – média responsabilidade em caso de crise, que se traduz numa ameaça moderada à reputação, incluindo desafios, acidentes por erros técnicos e defeitos de produto por erros técnicos; e c) intencional – forte responsabilidade em caso de crise, que se traduz numa ameaça grave à reputação, incluindo acidentes por erro humano, defeitos de produto por erro humano, comportamento inadequado da organização e má conduta organizacional (Coombs, 2007, p. 168). Quanto maior a responsabilidade atribuída a uma organização pela crise, maiores serão os danos à reputação, o que significa que as crises intencionais representam a ameaça mais grave, seguindo-se as crises acidentais e, por último, as crises de vítimas (Ma & Zhan, 2016, p. 12).

Tabela 2: Tipos de crise da Teoria Situacional de Comunicação de Crise (adaptado de Coombs, 2007)

Tipo de crise	**Nível de responsabilidade pela crise**	**Exemplos de crise**
Vítima	Responsabilidade baixa	● Desastres naturais ● Rumores ● Violência no local de trabalho ● Violação de produtos
Acidente	Responsabilidade média	● Desafios ● Acidentes por erros técnicos ● Defeitos de produto por erros técnicos
Intencional	Responsabilidade alta	● Acidentes por erro humano ● Defeitos de produto por erro humano ● Comportamento inadequado da organização ● Má conduta organizacional

A segunda etapa consiste em determinar se existe algum dos dois fatores de intensificação, nomeadamente: a) o histórico de crises – se uma organização teve ou não crises semelhantes no passado; e b) a reputação organizacional anterior à crise – a forma como a organização tem tratado os seus *stakeholders* no passado, ou seja, o estado geral da sua relação com os *stakeholders*

(Coombs & Holladay, 2010, p. 39). Acredita-se que as atribuições de responsabilidade em caso de crise se intensificam quando há um histórico de crises ou quando as relações com os *stakeholders* têm sido negativas, o que resulta numa ameaça à reputação organizacional (Coombs, 2004, p. 271).

Embora ambos os fatores tenham implicações na reputação organizacional em situação de crise, Coombs e Holladay (2001) referem que a reputação anterior à crise parece ter um efeito mais forte na atribuição de responsabilidade do que o histórico de crise (p. 337). Acredita-se que uma organização com uma reputação anterior favorável terá uma reputação pós-crise ainda mais forte, uma vez que tem mais capital de reputação a gastar do que uma organização com uma reputação anterior desfavorável ou neutra (Coombs & Holladay, 2006, p. 124).

Depois de avaliar as atribuições de responsabilidade em caso de crise, o gestor de crise escolhe, então, uma estratégia de resposta à crise adequada ao nível de responsabilidade pela crise (Coombs & Holladay, 2002, p. 169). A teoria situacional de comunicação de crise argumenta que cada resposta a uma crise deve começar com a informação de instrução e informação de ajustamento e, só depois, tentar esforços de reparação da reputação através das restantes estratégias de resposta (Coombs & Holladay, 2010, p. 40). Tal como afirma Park (2016), a utilização de respostas de base é importante não só porque satisfazem a necessidade de informação do público, mas também porque dão a impressão de que a organização dá prioridade à segurança do público e manifesta preocupação pelas vítimas (p. 3).

A teoria situacional de comunicação de crise divide as estratégias de resposta à crise em três categorias primárias: a) negação – prova que a crise não existiu ou que a organização não tem qualquer responsabilidade pela crise; b) diminuição – procura minimizar a responsabilidade da organização pela crise e/ou reduzir a perceção da gravidade da crise; e c) reconstrução – pretende melhorar a perceção da organização através de compensações e/ou pedidos de desculpa (Coombs & Holladay, 2010, pp. 40-41). Acrescenta-se uma estratégia complementar de reforço, utilizada para apoiar as três estratégias primárias, que procura divulgar informação positiva sobre a organização através de elogios ou relembrando as pessoas das boas ações passadas da organização (ibidem, 2010, p. 41).

Tabela 3: Estratégias de resposta da Teoria Situacional de Comunicação de Crise (adaptado de Coombs, 1999/2019)

Categoria de estratégia de resposta	**Subcategoria de estratégia de resposta**	**Definição**
Estratégia de negação	Atacar o acusador	O gestor de crise confronta a pessoa ou grupo que afirma existir uma crise. A resposta pode incluir uma ameaça de uso da força contra o acusador (por exemplo, um processo judicial).
	Negação	O gestor de crise afirma que não existe qualquer crise. A resposta pode incluir a explicação da razão pela qual não existe crise.
	Bode expiatório	Alguma outra pessoa ou grupo fora da organização é culpado pela crise.
Estratégia de diminuição	Escusa de responsabilidade	O gestor de crise tenta minimizar a responsabilidade da organização pela crise. A resposta pode incluir negar qualquer intenção de fazer mal ou afirmar que a organização não tinha qualquer controlo sobre os acontecimentos que conduziram à crise.
	Justificação	O gestor de crise tenta minimizar os danos percebidos associados à crise. A resposta pode incluir declarar que não houve danos ou ferimentos graves ou alegar que as vítimas mereceram o que receberam.
Estratégia de reconstrução	Compensação	A organização oferece dinheiro ou outra recompensa às vítimas.
	Pedido de desculpas	O gestor de crise declara publicamente que a organização assume plena responsabilidade pela crise e pede desculpa.
Estratégia de reforço	Recordação	A organização relembra os *stakeholders* das suas boas ações passadas.
	Ingratização	A organização elogia os *stakeholders*.
	Vítima	A organização explica como é também uma vítima da crise.

Quando a organização não tem qualquer responsabilidade pela crise, o gestor de crise deve utilizar a estratégia de negação e fornecer provas contra a perceção errónea de que a organização estava em crise (Coombs, 2014, p. 5). No caso da organização ter alguma responsabilidade pela

crise, são necessárias informações de instrução e de ajustamento para responder às necessidades das vítimas ou potenciais vítimas, devendo o gestor de crise enfatizar o que está a ser feito para ajudá-las (ibidem, 2014, p. 5). Caso a organização tenha uma grande responsabilidade pela crise, o gestor de crise deve começar por utilizar estratégias de informação de instrução e de ajustamento, acrescentando estratégias de reconstrução para maximizar o potencial de reparação da reputação (ibidem, 2014, p. 5).

De forma resumida, Coombs (1999/2019) sugere um conjunto de recomendações para a seleção da resposta adequada à crise, sendo elas (pp. 187-188):

- Fornecer a resposta de base ética sempre que houver vítimas ou potenciais vítimas, que inclui a informação de instrução sob a forma de avisos e orientações para as pessoas se protegerem dos danos, assim como a informação de ajustamento sob a forma de expressão de preocupações e ação corretiva;
- Utilizar estratégias de diminuição em crises de acidente e de vítima quando não existe historial de crise ou uma reputação anterior desfavorável;
- Utilizar estratégias de reconstrução em crises de acidente quando existe um historial de crise ou uma reputação anterior desfavorável;
- Utilizar estratégias de reconstrução para qualquer crise evitável;
- Utilizar estratégias de reforço como suplementos às restantes estratégias de resposta;
- A estratégia de resposta à vítima deve ser utilizada apenas com o grupo de vítimas;
- Não misturar estratégias de negação com estratégias de diminuição ou de reconstrução, por forma a demonstrar uma resposta consistente;
- As estratégias de diminuição e reconstrução podem ser utilizadas em combinação;
- A estratégia de negação apenas é utilizada quando existe desinformação e a organização não tem de facto qualquer ligação ou responsabilidade pela crise.

Segundo Claeys *et al.* (2010), a reputação organizacional é menos favorável quando as organizações são confrontadas com uma crise evitável, na medida em que são consideradas responsáveis pela crise (p. 261). Além disso, a reputação das organizações que utilizam estratégias de reconstrução é mais positiva do que a das organizações que priorizam as estratégias de diminuição (ibidem, 2010, p. 261).

3.4.3. Teoria de contingência

A teoria de contingência procura explicar como funcionam as Relações Públicas como um todo e como as organizações respondem perante situações de conflito, tendo por base um

continuum ancorado pela advocacia e pela acomodação (Coombs & Holladay, 2010, pp. 41-42). A advocacia é quando uma organização defende os seus próprios interesses, enquanto a acomodação é quando a organização faz concessões às outras partes (ibidem, 2010, p. 42).

Esta teoria identificou a ameaça como um fator situacional chave que influencia a postura de um profissional de Relações Públicas ao longo do continuum desde a advocacia à acomodação (Jin & Cameron, 2007, p. 262). Assim, é utilizado um modelo de avaliação da ameaça que conjuga o tipo da ameaça – interna ou externa à organização – e a duração da ameaça – curto ou longo prazo – para determinar o nível de ameaça (Coombs & Holladay, 2010, p. 43).

Ao nível dos efeitos do tipo de ameaça, Jin e Cameron (2007) concluíram que os profissionais de Relações Públicas em situações de crise perceberam exigências situacionais mais elevadas e projetaram mais recursos organizacionais necessários quando expostos a ameaças externas do que a ameaças internas (p. 272). Isto porque as ameaças externas pareciam colocar a organização sob maior perigo, exigindo mais esforços e impondo mais incerteza na tomada de decisões em situação de crise (ibidem, 2007, p. 272).

No que se refere aos efeitos da duração da ameaça, os resultados demonstraram que os profissionais de Relações Públicas perceberam maiores exigências situacionais e projetaram mais recursos organizacionais necessários quando expostos a ameaças a longo prazo do que a ameaças a curto prazo (Jin & Cameron, 2007, p. 274). Para uma organização em situação de crise, quanto mais tempo a ameaça se prolongar, mais exigente poderá ser controlá-la (ibidem, 2007, p. 274).

Capítulo II – O fenómeno dos ciberataques enquadrado na área das Relações Públicas

1. A emergência da Cibersegurança enquanto preocupação atual nas organizações

1.1. O conceito de Cibersegurança

Para melhor compreender o conceito de Cibersegurança, revela-se necessário entender o contexto em que o mesmo se aplica – o ciberespaço. Permitindo a interligação entre cerca de 2,7 milhões de pessoas em todo o mundo, o ciberespaço consiste num ambiente totalmente virtual, no qual ocorre troca de informação e comunicação tendo por base uma plataforma comum de partilha de ideias, serviços e relações, não existindo qualquer fronteira física ou política (Goutam, 2015, p. 14).

Segundo Singer e Friedman (2014), o ciberespaço é o primeiro e mais importante ambiente de informação, constituído por dados digitalizados que são criados, armazenados e, sobretudo, partilhados (p. 14). Contudo, o ciberespaço não é puramente virtual, compreendendo os computadores que armazenam os dados, bem como os sistemas e infraestruturas que permitem o seu fluxo, sustentados através da *Internet* (ibidem, 2014, p. 14). À semelhança do que acontece num contexto territorial, o ciberespaço depende da infraestrutura física e dos utilizadores humanos que estão ligados a nível geográfico e, por esse motivo, também está sujeito às noções humanas como soberania, nacionalidade e propriedade (ibidem, 2014, p. 14).

No contexto do ciberespaço, começam a emergir os ciberataques, que Denning e Denning (2010) definem como sendo ações deliberadas contra dados, *software* ou *hardware* em sistemas ou redes informáticas, com o intuito de destruir, perturbar, degradar ou negar o acesso ao utilizador (p. 29). Qualquer ataque informático cumpre três requisitos: acesso a um sistema ou uma rede; ocorrência de vulnerabilidades nos sistemas acedidos; e uma carga útil, que consiste num programa que executa ações uma vez encontrada e exercida uma vulnerabilidade (ibidem, 2010, p. 30).

Quando comparado com um ataque tradicional, um ciberataque distingue-se pela utilização dos meios digitais, podendo mover-se literalmente à velocidade da luz, não limitado pela geografia e pelas fronteiras físicas (Singer & Friedman, 2014, pp. 68-69). Dado que não é limitado pela física habitual dos ataques tradicionais, pode também ocorrer em múltiplos lugares ao mesmo tempo, o que significa que o mesmo ataque pode atingir diferentes alvos simultaneamente (ibidem, 2014, p. 69). De notar ainda que, em vez de causar danos físicos diretos, um ciberataque visa sempre primeiro outro computador e a informação nele contida, embora, numa segunda fase, possa resultar efetivamente em danos de natureza física para o utilizador (ibidem, 2014, p. 69).

Por sua vez, Hussain *et al.* (2020) acreditam que os ciberataques podem ser traduzidos em todas as atividades ilegais que estão a ser realizadas no ciberespaço (p. 2). Desde o ataque a um utilizador individual até uma rede de organizações violadoras, passando também pelo roubo de dados, existem inúmeros tipos de cibercrimes que estão a ocorrer atualmente (ibidem, 2020, p. 2). Segundo Kuipers e Schonheit (2021), as violações de dados *online* representam um dos incidentes cibernéticos mais recorrentes e prejudiciais para as organizações em todo o mundo (p. 2).

Na sequência da emergência dos ciberataques, surge a Cibersegurança, definida como sendo a organização e recolha de recursos, processos e estruturas utilizadas para proteger o ciberespaço, bem como os sistemas habilitados para o ciberespaço, de ocorrências que desalinham os direitos de propriedade (Craigen *et al.*, 2014, p. 17).

Através da conjugação de diferentes definições apresentadas por diversos autores, Schatz *et al.* (2017) sugerem a seguinte definição de Cibersegurança:

> *A abordagem e as ações associadas aos processos de gestão dos riscos de segurança seguidos pelas organizações e estados para proteger a confidencialidade, integridade e disponibilidade dos dados e bens utilizados no ciberespaço. O conceito inclui diretrizes, políticas e coleções de salvaguardas, tecnologias, ferramentas e formação para proporcionar a melhor proteção para o estado do ambiente cibernético e dos seus utilizadores* (Schatz *et al.*, 2017, p. 66)

De acordo com Tanenbaum e Wetherall (2011), a Cibersegurança apresenta um conjunto de propósitos, nomeadamente (p. 763):

- Preocupa-se em garantir que terceiros não consigam ler ou modificar secretamente mensagens destinadas a outros recetores; preocupa-se em evitar que terceiros tentem aceder remotamente a serviços a que não estão autorizados a utilizar;
- Preocupa-se em arranjar maneiras de verificar se uma mensagem alegadamente das finanças é realmente das finanças e não de uma organização criminosa;
- Lida com problemas de captura e reprodução de mensagens legítimas, e com pessoas que mais tarde tentam negar o envio dessas mesmas mensagens.

Importa mencionar, ainda, que a maioria dos problemas de segurança é intencionalmente causada por pessoas maliciosas que tentam obter algum benefício, chamar a atenção ou prejudicar alguém (Tanenbaum & Wetherall, 2011, pp. 763-764).

Posto isto, os problemas de Cibersegurança podem ser divididos em quatro áreas estreitamente interligadas, sendo elas (Tanenbaum & Wetherall, 2011, p. 764):

a) O sigilo, também denominado confidencialidade, que procura manter a informação afastada dos utilizadores não autorizados;
b) A autenticação, que trata de determinar com quem se está a falar antes de revelar informações confidenciais ou entrar num acordo comercial;
c) O não-repúdio, através da utilização de assinaturas que comprovem o consentimento da outra parte;
d) O controlo de integridade, que garante a autenticidade da mensagem recebida.

Embora o conceito de Cibersegurança seja distinto do conceito de Segurança da Informação, von Solms e van Niekerk (2013) defendem uma interligação entre eles. Por um lado,

a Segurança de Informação engloba a proteção dos bens das Tecnologias de Informação e Comunicação (TIC) subjacentes, indo além da tecnologia para incluir também a informação que não é armazenada ou comunicada diretamente através da utilização das TIC (ibidem, 2013, p. 4). Neste caso, a informação e as TIC constituem-se como a causa subjacente da vulnerabilidade (ibidem, 2013, p. 4). Em contrapartida, a Cibersegurança implica a proteção de bens que podem variar desde a pessoa em si até aos aparelhos domésticos comuns, aos interesses da sociedade em geral, incluindo infraestruturas nacionais críticas, devido às vulnerabilidades que existem como resultado da utilização das TIC que constituem a base de funcionamento do ciberespaço (ibidem, 2013, p. 4). Em função desta distinção e dos cenários anteriormente explorados, é evidente que na Cibersegurança o bem que precisa essencialmente de ser protegido ultrapassa os limites da informação em si, tal como definido para a Segurança da Informação (ibidem, 2013, p. 4)

É neste sentido que von Solms e von Solms (2018) propõem uma definição para o conceito de Cibersegurança:

> *Parte da Segurança da Informação que se concentra especificamente na proteção da Confidencialidade, Integridade e Disponibilidade (CID) dos bens de informação digital contra quaisquer ameaças que possam surgir do facto de tais bens estarem comprometidos através da utilização da Internet* (von Solms & von Solms, 2018, p. 5)

Ao tentar compreender o âmbito da Cibersegurança, Hussain *et al.* (2020) sublinham que, embora estejamos a beneficiar da evolução e rápida expansão da tecnologia, estamos a integrar estas mudanças na Infraestrutura Crítica – sistema principal que atua como o corpo de todos os sistemas, redes e bens essenciais para a segurança e proteção de um país, segurança pública e economia, sendo o seu funcionamento contínuo e sem obstáculos uma obrigação (p. 2). Significa isto que a Cibersegurança não só reflete o estado de segurança de uma organização, mas também o estado de segurança do próprio país (ibidem, 2020, p. 2).

Numa tentativa de esclarecer a definição de Cibersegurança, Aslan *et al.* (2023) apresentam as três dimensões que integram o conceito (p. 8). A primeira dimensão, conhecida como "princípio da segurança da informação", inclui os conceitos de confidencialidade, integridade e disponibilidade, sendo utilizada para proteger a informação dos *hackers* (ibidem, 2023, p. 8). A segunda dimensão visa proteger os dados em todos os estados, seja em armazenamento, transporte ou processo, o que significa que as medidas de cibersegurança devem assegurar a confidencialidade, integridade e disponibilidade dos dados quando estes são armazenados ou transmitidos entre dispositivos de rede e *hosts* (ibidem, 2023, p. 8). A última dimensão envolve a

utilização de ferramentas adicionais, tais como políticas e práticas, novas tecnologias e sensibilização dos utilizadores para ajudar a proteger o ciberespaço (ibidem, 2023, p. 8).

Posto isto, de acordo com a Associação para a Promoção e Desenvolvimento da Sociedade de Informação (2023), importa esclarecer alguns conceitos relacionados com a Cibersegurança, apresentados na Tabela 4.

Tabela 4: Conceitos relacionados com a Cibersegurança

Conceito	**Definição**
Ameaça	Ação ou evento que tem como objetivo comprometer a segurança
Autenticação de identidade	Verificação ou validação da identidade de uma pessoa ou da identificação de qualquer outra entidade através de um sistema de segurança
Autenticação de mensagem	Processo de validar o código de autenticação de uma mensagem, para obter a garantia de que um dado remetente emitiu essa mensagem para o destinatário previsto e de que a mesma não sofreu alterações durante a transmissão
Autenticidade	Num contexto informacional, propriedade de uma informação cuja origem e integridade são garantidas
Cibercrime	Qualquer tipo de crime perpetrado na *Internet* ou nas novas redes de telecomunicações, cada vez mais acessíveis em termos de custo e de facilidade de acesso
Ciberética	Conjunto das regras morais e consequentes regras de conduta que devem reger os navegadores no ciberespaço, mais concretamente os utilizadores da *Internet*
Ciberguerra	Modalidade de guerra onde a conflitualidade não ocorre com armas físicas, mas através da confrontação com meios eletrónicos e informáticos no chamado ciberespaço
Certificação	Processo pelo qual uma entidade competente assegura, normalmente por escrito, que um sistema, produto ou componente está conforme com as especificações técnicas de funcionamento ou de segurança estabelecidas e que portanto pode ser usado sem problemas
Confidencialidade	No caso da informação, diz-se confidencial a informação cujo acesso é restrito a um grupo de entidades (utilizadores ou programas) que possuem os privilégios necessários para conhecer/utilizar essa informação
Dark Web	Pequena parte dos conteúdos da web profunda, para os quais é necessário introduzir credenciais para

	aceder ou que foram intencionalmente ocultos da indexação dos motores de busca
Deep Web	Refere-se aos conteúdos existentes na *Internet* que não são acessíveis pelos habituais navegadores web ou que não são indexados pelos motores de busca. Estes conteúdos podem ser de origem diversa, e incluem páginas web que são geradas no momento em que se acede a uma base de dados específica para consultar/obter informação
Disponibilidade	Em tecnologias da informação e da comunicação, capacidade de uma unidade funcional permanecer em estado de realizar uma determinada função dentro de condições determinadas, num dado instante ou num dado intervalo de tempo, supondo que estão assegurados os necessários meios exteriores
Integridade	Garantia de que os dados ou a informação não sejam alterados de modo não autorizado
Segurança Informática	Tomada de um conjunto de medidas de segurança (físicas, lógicas e administrativas) e de medidas de urgência em caso de situações imprevistas, de forma a assegurar a proteção dos bens informáticos de uma organização (*hardware*, *software* e dados), assim como a continuidade do serviço
Vulnerabilidade	Fraqueza de um sistema informático, revelada por um exame à sua segurança (por exemplo, devido a falhas na análise, conceção, implementação ou operação), que se traduz por uma incapacidade de fazer frente às ameaças informáticas que pesam sobre ele

1.2. Contexto histórico

Em termos de enquadramento histórico, Alexandrou (2021) propõe quatro fases de evolução do cibercrime, sendo elas: Fase Experimental, Pré-Cibercrime, Fase de Desenvolvimento do Cibercrime e Guerra Cibernética promovida pelo Estado (p. 59). Importa referir que o início de uma nova fase não assinala o fim da anterior, funcionando apenas como um contributo para a história da cibercriminalidade (ibidem, 2021, p. 59).

A primeira fase, que decorre entre 1970 e 1980, denomina-se Fase Experimental, no sentido em que se verifica um esforço exploratório ou experimental para controlar situações à distância, utilizando tecnologia informática (Alexandrou, 2021, p. 59). Esta fase inicia-se na década de 70 com o surgimento do primeiro *worm*, denominado *Creeper*, constituindo-se como a primeira tentativa ilegal de alterar um programa de *software* para transmitir uma mensagem específica, embora não tenha prejudicado ou alterado quaisquer dados (ibidem, 2021, p. 60). Entre o conjunto de ferramentas que começaram a emergir neste período, incluem-se os códigos maliciosos, *trojans*, *worms* avançados e vírus que replicam e colidem com sistemas ou ficheiros

danificados (ibidem, 2021, p. 60). Uma das inovações mais importantes desta época foi o desenvolvimento e utilização do correio eletrónico, sendo que, até à data, os *e-mails* eram concebidos para entregar mensagens e ficheiros diretamente aos impressores (ibidem, 2021, p. 60). O termo *hacking* teve origem nos anos 60 enquanto termo utilizado para divertimento e reconhecimento – e não para atividade ilegal –, ainda que, em 1984, o Congresso dos EUA tenha aprovado a primeira legislação relacionada com o conceito, nomeadamente a Lei de Fraude e Abuso de Computadores (ibidem, 2021, p. 61). Em 1988, o famoso *Morris worm* multiplicou-se milhares de vezes através de uma enorme rede de computadores de várias universidades até colapsar o sistema, ficando conhecido como o primeiro *worm* da *Internet* (ibidem, 2021, p. 62).

A segunda fase, intitulada Pré-Cibercrime, começa no início de 1990 e estende-se até ao ano 2000, caracterizada pela formação de grupos de *hacking* e pela criação de alguns vírus e *worms* altamente eficazes, destinados a paralisar grandes sistemas (Alexandrou, 2021, p. 59). Com o avanço dos programas *Web* nos anos 90, tornou-se mais fácil enviar vírus através de ligações à *Internet*, fazendo com que os computadores funcionassem mais lentamente e permitindo o aparecimento de anúncios *pop-up* (ibidem, 2021, p. 62). A título exemplificativo, destacam-se o vírus *Michelangelo*, que apareceu em 1991, considerado o primeiro *malware* público da história, bem como o vírus *Melissa*, que apareceu em 1999, espalhando-se entre milhões de *e-mails* de clientes da Microsoft (ibidem, 2021, p. 62).

Com origem no início dos anos 2000 e estendendo-se até 2010, segue-se a terceira fase, denominada Fase de Desenvolvimento do Cibercrime, caracterizada pela adoção generalizada da tecnologia da *Internet* e pela utilização das redes sociais, resultando em crimes que são, na sua maioria, financeiros (Alexandrou, 2021, p. 59). Após estabelecerem a *Internet* como o seu principal canal de comunicação e comércio eletrónico ilegal, os *hackers* começaram a visar os grandes dados através de crimes monetários, incluindo roubo de identidade e cartões de crédito, *phishing*, ataques DNS (*Domain Name Server*), *botnets* e utilização de *ransomware* e *spyware* (ibidem, 2021, p. 63). Devido à proliferação da tecnologia e à rápida disseminação de dispositivos móveis, o número e a tipologia de ataques *online* cresceram exponencialmente, traduzindo-se em grandes ataques DDoS (*Distributed Denial of Service*) em empresas como a Amazon, a CNN, a eBay ou o Yahoo (ibidem, 2021, p. 63). Importa mencionar, também, os três avanços tecnológicos notáveis que mudaram a forma como as pessoas interagem entre si, nomeadamente o *Apple iPhone*, introduzido pela primeira vez em 2007, o *Android Operating System*, introduzido em 2008, e o *Cloud Computing* (ibidem, 2021, pp. 65-66). Contudo, uma grande preocupação relacionada com o *cloud computing* tem sido a questão da segurança e da privacidade dos dados, proporcionando o aumento do número de ciberataques (ibidem, 2021, p. 66). Entre os diversos

vírus que se espalharam pela *Internet* durante esta fase, destacam-se o *ILOVEYOU vírus*, o *Klez worm*, o *Sobig worm*, o *Mydoom worm*, o *Sober email worm*, o *Zeus vírus*, o *SpyEye malware* e o *Sutxnet worm* (ibidem, 2021, pp. 63-67).

Por último, Alexandrou (2021) denomina a quarta fase de Guerra Cibernética promovida pelo Estado, a qual teve início em 2011, estendendo-se até à atualidade (p. 59). Esta fase compreende, essencialmente, ciberataques patrocinados pelo Estado, espionagem, violações da privacidade e confidencialidade do governo, e a manipulação da opinião pública através da persuasão sobre as plataformas dos *media* (ibidem, 2021, p. 67). Durante este período, começam também a emergir as *fake news* e assiste-se ao fim da privacidade pessoal, comprovando a teoria de George Orwell, no seu romance *1984*, sobre vivermos na era da vigilância (ibidem, 2021, p. 67). Além disso, durante esta fase, continua a verificar-se a ocorrência de formas mais antigas de cibercrime, como sendo o *malware* bancário, roubo de carteiras de *bitcoin*, *hacks* de dispositivos móveis e extorsão através de ataques *ransomware* (ibidem, 2021, p. 71). Com a fusão entre ameaças novas e antigas, o cibercrime começa a crescer para além do *hacking* e roubo de identidade, transformando-se numa ameaça global mais sofisticada e assemelhando-se a uma silenciosa guerra mundial, que não conhece fronteiras e que diz respeito a todas as nações do planeta (ibidem, 2021, p. 71). Entre os vários incidentes que se desencadearam nesta fase, destacam-se o *Mirai malware*, que despoletou em 2016, e o ataque de *ransomware WannaCry*, que decorreu em 2017 (ibidem. 2021, p. 71).

A guerra cibernética pode ser definida como sendo uma extensão da política através de ações empreendidas no ciberespaço por atores estatais ou não estatais que ou constituem uma ameaça grave à segurança de uma nação ou são conduzidas em resposta a uma ameaça percebida contra a segurança de uma nação (Shakarian *et al.*, 2013, p. 2). Embora exista alguma ambiguidade na definição do conceito de guerra cibernética, Singer e Friedman (2014) procuram descomplicar acreditando que os elementos-chave de uma guerra cibernética têm todos os paralelos e ligações com a guerra noutros domínios, ou seja, a guerra tem sempre um objetivo, um carácter político e um elemento de violência, seja em terra, no mar ou no ciberespaço (p. 121).

Por sua vez, Holland (2022) acredita que na primeira fase de evolução da cibercriminalidade, com início em 1990 e término em 2006, as comunidades de *hackers* globais começaram a formar-se, partilhando façanhas e técnicas de ataque, enquanto grupos e indivíduos demonstraram as suas capacidades técnicas como forma de se vangloriar, sendo que os ataques, normalmente, não eram motivados financeiramente (p. 6). Na segunda fase, compreendida entre 2006 e 2013, o desenvolvimento de ataques de *malware* começou a baixar os níveis de

competências necessárias para a entrada no mercado do cibercrime, levando os *hackers* a reunir os seus pontos fortes em novas redes, especializando-se em áreas específicas, que se centravam na fraude e que visavam os utilizadores de bancos *online* em detrimento de empresas (ibidem, 2022, p. 7). Segue-se a terceira fase, compreendida entre 2010 e 2018, em que os ataques informáticos passaram da fraude para a negação de dados e ataques destrutivos, enquanto o *ransomware* começou a destacar-se como o método de valorização monetária (ibidem, 2022, p, 9). Além disso, nesta fase, os *hackers* estavam a começar a oferecer *Malware as a Service* (MaaS), vendendo produtos e serviços especializados (ibidem, 2022, p. 9). Na última fase, com início em 2018 e que decorre até à atualidade, o cibercrime tem continuado a sua tendência para modelos de negócio de serviços e plataformas, começando os *hackers* a explorar cadeias de fornecimento complexas para lançar ataques utilizando componentes especializados "*plug and play*" (ibidem, 2022, p. 11). Adicionalmente, o cibercrime está a tornar-se mais organizado e direcionado, visto que os *hackers* estão a levar muito mais tempo a compreender a infraestrutura de um alvo para maximizar o seu impacto, quer isso se traduza em obter um resgate maior ou incapacitar uma peça de infraestrutura mais crítica (ibidem, 2022, p. 11).

A verdade é que, nos últimos anos, a importância e utilização da *Internet* aumentaram rapidamente em todo o mundo, resultando na transferência da vida quotidiana para o mundo digital (Aslan *et al.*, 2023, p. 10). A pandemia provocada pela Covid-19 veio acelerar este processo, fazendo com que as pessoas desenvolvam relações através dos meios digitais, acedam a sistemas bancários digitais ou planeiam as suas reuniões *online* (ibidem, 2023, p. 10). Estas razões conduziram igualmente à transferência de crimes diários para a *Internet* (ibidem, 2023, p. 10).

Ao nível da tipologia da cibercriminalidade, Alexandrou (2021) define três categorias: cibercriminalidade contra o governo, cibercriminalidade contra organizações ou contra bens e cibercriminalidade contra indivíduos (p. 73). No que se refere à cibercriminalidade contra o governo, estamos perante um ataque contra a soberania de um estado ou nação que se traduz numa tentativa de limitar o seu poder, incluindo a invasão de *websites* governamentais, militares ou de fornecedores de defesa, ataques contra infraestruturas críticas, distribuição de *malware*, ataques de negação de serviço (DoS e DDoS) e ataques de *ransomware* (ibidem, 2021, p. 74). Por sua vez, a cibercriminalidade contra organizações ou contra bens caracteriza-se pela intrusão não autorizada de computadores na informação privada de qualquer empresa ou propriedade, incluindo transferência não autorizada, roubo ou posse de dados, utilização de um computador ou rede sem autorização, vandalismo informático ou de rede e ataques que utilizem *software* malicioso, como *spyware*, *ransomware*, *malware* e *keylogger* (ibidem, 2021, p. 74). Por último, a cibercriminalidade contra indivíduos envolve um crime informático que tem como alvo um

indivíduo, incluindo a utilização de *malware*, *ransomware*, *hacking*, *spamming*, *phishing*, roubo de identidade e esquemas *online*, bem como extorsão, *cyberbullying*, ciberperseguição, assédio cibernético, difamação ou calúnia *online*, *sexting* e distribuição de pornografia infantil ou outro material pornográfico (ibidem, 2021, p. 75).

Por sua vez, Chng *et al.* (2022) enumeram um conjunto de motivações para a ocorrência de ciberataques, em função do tipo de *hacker* (pp. 3-6), como é possível verificar na Tabela 5.

Tabela 5: Motivações para a ocorrência de ciberataques, em função do tipo de *hacker*

Tipo de *hacker*	**Definição**	**Motivações**
Novatos	*Hackers* menos qualificados e que dependem fortemente de *kits* de ferramentas *online* desenvolvidos e fornecidos por terceiros	● Curiosidade ● Notoriedade ● Lazer
Cyberpunks	*Hackers* de baixa a média qualificação que causam danos por diversão	● Ganhos financeiros ● Notoriedade ● Vingança ● Lazer
Infiltrados	Colaboradores insatisfeitos ou ex-colaboradores de uma organização que abusam do seu acesso interno para obter o que pretendem	● Ganhos financeiros ● Vingança ● Ideologia
Old guards (guardas antigos)	*Hackers* não maliciosos, que não têm respeito pela privacidade pessoal	● Curiosidade ● Notoriedade ● Lazer ● Ideologia
Profissionais	Indivíduos altamente qualificados que são pagos para cometer um crime	● Ganhos financeiros ● Vingança
Hacktivistas	Também conhecidos como ativistas políticos, usam as suas capacidades técnicas para promover as suas agendas políticas através da *Internet*	● Notoriedade ● Vingança ● Lazer ● Ideologia
Hackers dos Estados-Nação	Indivíduos altamente treinados e extremamente qualificados, como sendo os ciberterroristas e os atores estatais, que trabalham direta ou indiretamente para desestabilizar, perturbar e destruir os sistemas e redes de uma nação ou governo	● Ganhos financeiros ● Vingança ● Ideologia
Estudantes	Não têm qualquer intenção de *hackear*, fazendo-o apenas para ganhar conhecimento	● Curiosidade
Petty Thieves (Pequenos ladrões)	Indivíduos, incluindo burlões e extorsionistas, que promovem as suas atividades ilegais *online*	● Ganhos financeiros ● Vingança
Piratas digitais	Também conhecidos como violadores	● Ganhos financeiros

	de direitos de autor, possuem e promovem cópias ilegais, bem como a distribuição, *download* ou venda de materiais protegidos por direitos de autor	
Agressores sexuais *online*	Indivíduos, incluindo os predadores sexuais e pedófilos, que utilizam abusivamente a *Internet* para se envolverem em comportamentos sexualmente desviantes com crianças	● Impulsos sexuais
Crowdsourcers	Indivíduos que se juntam para resolver um problema, frequentemente utilizando métodos questionáveis ou perseguindo objetivos duvidosos	● Notoriedade ● Vingança ● Lazer ● Ideologia
Mediadores do crime	Indivíduos que fornecem as ferramentas e os conhecimentos técnicos necessários aos cibercriminosos, permitindo-lhes lançar ataques sofisticados que de outra forma não teriam sido possíveis	● Ganhos financeiros

1.3. Quadro legal

1.3.1. Contexto internacional

A nível internacional, o Conselho da Europa aprovou, em novembro de 2001, a Convenção de Budapeste sobre Cibercrime, com o intuito de harmonizar a legislação sobre cibercrime e melhorar a cooperação internacional, através de uma política comum e alinhada entre os países aderentes (Carballo-Cruz, 2022, p. 51). Constituindo-se como um importante instrumento internacional vinculante sobre cibercrime, a Convenção foi ratificada, até 2021, por 66 Estados, 45 membros do Conselho da Europa e 21 não-membros (ibidem, 2022, p. 51). Entre os crimes que a Convenção prevê, incluem-se o acesso e a interceção ilegítimos, a interferência em dados e sistemas, o uso indevido de dispositivos, a falsidade e a burla informática, a pornografia infantil, o dano e a sabotagem informática ou a utilização de vírus (Barros, 2018, p. 38).

Em 2007, a União Internacional de Telecomunicações (ITU), organismo integrado nas Nações Unidas, lançou a Agenda Global da Cibersegurança (GCA) enquanto quadro de referência para a cooperação internacional em matéria de cibersegurança (Carballo-Cruz, 2022, p. 52). Entre os principais projetos desenvolvidos pela ITU, incluem-se: a) a elaboração de estratégias de cibersegurança e a sua publicação; b) a constituição de equipas de resposta a incidentes informáticos (CSIRT); c) a definição de iniciativas para melhorar a preparação, a proteção e as capacidades de resposta a ciberataques; e d) a realização anual do Índice Global Cibersegurança (GCI), com o intuito de medir o compromisso dos países com a segurança cibernética (ibidem, 2022, p. 52).

A verdade é que a cibersegurança se constitui como uma área de crescente interesse para as Nações Unidas, pelo que a instituição tem vindo a desenvolver um conjunto de iniciativas nesse contexto, nomeadamente: a) o debate sobre as ameaças à segurança da informação promovido pelo Comité para o Desarmamento e a Segurança Internacional; b) a adoção de resoluções associadas à cibersegurança por parte do Comité para as Questões Sociais, Humanitárias e Culturais e do Comité Económico e Financeiro; c) o desenvolvimento do programa de Cibersegurança e Novas Tecnologias, que tem como objetivo auxiliar os Estados-membros e as organizações privadas na sua capacidade de antecipar e reduzir a utilização da tecnologia por parte dos *hackers*; d) a criação de um contexto digital mais seguro, através da criação de um Relator Especial sobre o direito à privacidade; e e) o aumento do interesse relativamente à área da cibersegurança por parte do Conselho Económico e Social e do Congresso das Nações Unidas sobre Prevenção da Criminalidade e Justiça Criminal (Carballo-Cruz, 2022, p. 51).

A Organização para a Cooperação e o Desenvolvimento (OCDE) é outra instituição internacional que se preocupa com as questões inerentes à cibersegurança, apoiando-se num Grupo de Trabalho sobre Segurança na Economia Digital, cujo principal objetivo passa por desenvolver e promover políticas que reforcem a segurança da economia digital (Carballo-Cruz, 2022, p. 52). Em 2018, a OCDE desenvolveu o Fórum Global sobre Segurança Digital para a Prosperidade, uma iniciativa de carácter internacional, multilateral e multidisciplinar que promove o intercâmbio de experiências e boas práticas no que toca aos riscos da segurança digital, além de proporcionar uma aprendizagem conjunta e a criação de convergências na área (ibidem, 2022, p. 52).

Devido ao papel fundamental que detém na defesa de conflitos e situações de guerra entre países, a Organização para o Tratado do Atlântico Norte (NATO) é apontada como um dos organismos internacionais que mais iniciativas tem desenvolvido no contexto do ciberespaço (Carballo-Cruz, 2022, p. 52). Em 2008, criou um Centro de Excelência de Defesa do Ciberespaço, localizado em Talin, com o intuito de promover a investigação e formação na área da cibersegurança, organizando periodicamente exercícios dedicados à ciberdefesa (ibidem, 2022, p. 52). Destaca-se o *Locked Shields* como o maior exercício realizado neste contexto, contando com a participação de mais de 2.000 pessoas (ibidem, 2022, p. 52).

No âmbito da NATO, foi lançada, em 2012, a Agência de Comunicações e Informações, sediada em Bruxelas, que tem como principal finalidade proteger as redes e infraestruturas de comunicação e informação da Aliança e dos seus membros (Carballo-Cruz, 2022, p. 53). Integrado na Agência, foi desenvolvido um Centro de Cibersegurança que funciona como um *ciberhub* para a partilha de informação e conhecimento entre os membros da NATO, disponibilizando serviços

especializados para antecipar, detetar, responder e recuperar de ciberataques (ibidem, 2022, p. 53). Em 2019, a Agência criou a rede de Equipas de Resposta a Emergências Informáticas da NATO (ibidem, 2022, p. 53).

Em conjunto com a União Europeia, a NATO criou, em 2017, o Centro de Excelência no Combate a Ameaças Híbridas (*Hybrid CoE*), sediado em Helsínquia (Carballo-Cruz, 2022, p. 53). Adicionalmente, foi estabelecido, em 2018, um Centro de Operações do Ciberespaço, com sede em Bruxelas, por forma a garantir uma maior coordenação operacional, fortalecer a cibersegurança e incorporar o ciberespaço nas operações de defesa da NATO (ibidem, 2022, p. 53).

Sendo um dos principais organismos de defesa a nível internacional, a NATO compromete-se com a utilização das suas capacidades para responder e defender-se perante qualquer tipo de ameaça cibernética, pelo que, no âmbito do quadro da sua Agenda 2030, tem como objetivo reforçar o ciberespaço como principal domínio de intervenção nos próximos anos (Carballo-Cruz, 2022, p. 53).

1.3.2. Contexto europeu

O quadro legislativo e institucional da União Europeia constitui-se como fundamental para reforçar a cibersegurança a nível macro, reduzir a incerteza para a generalidade dos agentes económicos e conferir segurança jurídica às empresas e aos cidadãos (Carballo-Cruz, 2022, p. 44).

Em 2013, a União Europeia publicou o primeiro documento estratégico sobre cibersegurança, intitulado *Estratégia de Cibersegurança na União Europeia: um ciberespaço aberto, seguro e protegido*, o qual previa um papel central dos governos em matéria de prevenção e resposta aos ciberataques, contrariamente à abordagem de cooperação internacional e colaboração com o setor privado defendidas atualmente (Carballo-Cruz, 2022, p. 44). Esta estratégia foi revista em setembro de 2017, resultando na aprovação do Pacote de Cibersegurança, que tinha como objetivo proteger os cidadãos e as empresas em matéria de propriedade intelectual e dados pessoais, e no qual estava incluída a denominada *Cibersecurity Act* (ibidem, 2022, p. 45).

Perante a necessidade de reforçar a cooperação entre os Estados-membros, foi publicada, em 2016, a Diretiva sobre a Segurança de Redes e Sistemas de Informação (Diretiva SRI), considerada a peça fundamental em matéria de cibersegurança na União Europeia (Carballo-Cruz, 2022, p. 44). Na presente Diretiva, estavam consagrados os seguintes objetivos: a) adotar uma estratégia nacional de segurança das redes e dos sistemas de informação; b) melhorar a cooperação estratégica e o intercâmbio de informações entre os Estados-membros; c) criar uma rede de equipas

de resposta a incidentes de segurança cibernética – a rede de CSIRT; d) estabelecer requisitos de segurança e de notificação para os operadores de serviços essenciais e para os prestadores de serviços digitais; e e) designar as autoridades nacionais competentes, os pontos de contacto únicos e as CSIRT com atribuições no âmbito da segurança das redes e dos sistemas de informação (n.º 2 do artigo 1º da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho).

Por forma a reforçar o papel da Agência de Cibersegurança da União Europeia (ENISA), o Parlamento Europeu, o Conselho Europeu e a Comissão Europeia estabeleceram, em dezembro de 2018, um acordo político sobre a *Cibersecurity Act*, a qual definiu, simultaneamente, um quadro europeu para a certificação a respeito de cibersegurança de serviços *online* e aparelhos eletrónicos (Carballo-Cruz, 2022, p. 45).

Na sequência do acordo sobre a *Cibersecurity Act*, foi aprovado, em abril de 2019, o Regulamento relativo à ENISA e à certificação da cibersegurança das TIC (Carballo-Cruz, 2022, p. 45). Além de renovar o mandato da ENISA, estabelecendo os seus objetivos, atribuições e aspetos organizativos, o regulamento prevê um enquadramento para a certificação da cibersegurança no que respeita a produtos, serviços e processos digitais, válido em toda a União Europeia (n.º 1 do artigo 1º do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho). Segundo Carballo-Cruz (2022), este referencial de certificação é um elemento fundamental do Mercado Único Digital, que pretende gerar confiança, acelerar o crescimento do mercado da cibersegurança e facilitar o comércio na União Europeia (p. 45).

Ainda em 2019, o Conselho Europeu desenvolveu um quadro que permite à União Europeia impor sanções para impedir a ocorrência de ciberataques que se constituam como uma ameaça para o contexto europeu e, inclusive, responder a essas agressões (Carballo-Cruz, 2022, p. 45). Entre o conjunto de sanções estabelecidas, prevê-se a proibição de entrada na União Europeia, no caso de cidadãos europeus responsáveis por ciberataques, ou a imobilização de ativos (ibidem, 2022, p. 45).

Posteriormente, em dezembro de 2020, a Comissão Europeia aprovou um conjunto de medidas com o intuito de adaptar o quadro europeu de cibersegurança à transformação digital (Carballo-Cruz, 2022, pp. 45-47), entre as quais se destacam:

- Estratégia de Cibersegurança da União Europeia para a Década Digital, que tem como objetivo reforçar a resiliência das cibercomunidades da União Europeia, nomeadamente o mercado, a diplomacia, a segurança e a defesa, promovendo igualmente o desenvolvimento de soluções em diversos âmbitos, como a ciberdefesa e a segurança da *Internet*, bem a

definição de um regulamento sobre segurança da IoT (*Internet of Things*) (ibidem, 2022, pp. 45-47);

- Proposta de revisão da Diretiva de Segurança de Redes e Sistemas de Informação (SRI 2.0) (Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho), no sentido de reforçar as obrigações de segurança das empresas, melhorar a segurança das cadeias de fornecimento, estabelecer medidas de supervisão mais rigorosas para as autoridades nacionais, incluindo a aplicação de coimas por incumprimento de normas, e estimular as trocas de informação e cooperação (ibidem, 2022, pp. 45-47);
- Proposta de Diretiva sobre Resiliência de Entidades Críticas, que substitua a Diretiva de Proteção de Infraestruturas Críticas, de 2008 (Diretiva 2008/114/CE do Conselho), cujo intuito é aumentar o seu âmbito de aplicação – passando de dois para dez setores –, bem como alargar a sua abrangência funcional, ao substituir infraestruturas críticas por entidades críticas (ibidem, 2022, pp. 45-47);
- Inclusão da cibersegurança nos fundos *Repair* e *Prepare* do pacote *Next Generation*, uma vez que os recursos destinados à recuperação pós-pandémica têm como objetivo promover a transformação estrutural da economia europeia e, para o efeito, é imprescindível desenvolver os instrumentos e níveis de cibersegurança (ibidem, 2022, pp. 45-47).

De mencionar que, para 2021 e anos seguintes, a Comissão Europeia aprovou uma agenda que contempla um conjunto de iniciativas, nomeadamente: a) a implementação de medidas relativas à cibersegurança de redes 5G (*EU Toolkit Box*); b) a criação da Unidade Conjunta de Cibersegurança (*Joint Cyber Unit*) para a coordenação operacional dos Estados-membros; c) a designação de referenciais de certificação (*EU Cibersecurity Act*); d) a regulação do acesso a comunicações cifradas com o intuito de compatibilizar a privacidade e a interceção legal de comunicações; e) a revisão da Diretiva de Privacidade Eletrónica; e f) a aceleração do investimento no período 2021-2027, através dos programas Europa Digital e Horizonte Europa e do Plano de Recuperação para a Europa (Carballo-Cruz, 2022, p. 47).

Em termos de segurança e privacidade dos dados, a União Europeia tem desenvolvido, além da legislação em vigor, diversos diplomas, entre os quais estão contemplados: o Regulamento Geral sobre a Proteção de Dados, em vigor desde 2018 (Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho), que permite aos cidadãos ter um maior controlo sobre os seus dados pessoais; a Diretiva de Privacidade Eletrónica, em vigor desde 2002 (Diretiva 2002/58/CE do Parlamento Europeu e do Conselho), que assegura a confidencialidade das comunicações, estabelecendo as regras de rastreio e monitorização *online*; e a Regulamentação do eIDAS – Sistema de Identificação e Autenticação Eletrónica à escala Europeia, em vigor desde 2018

(Regulamento (EU) 2014/910 do Parlamento Europeu e do Conselho), que permite aos particulares e às empresas a realização das suas transações eletrónicas de forma segura e confiável (Carballo-Cruz, 2022, p. 47).

1.3.3. Contexto português

No caso específico do contexto português, o enquadramento institucional e normativo da Cibersegurança é, em larga medida, influenciado pela legislação em vigor na União Europeia (Carballo-Cruz, 2022, p. 49). Sendo Portugal membro da União Europeia, assim como de organizações internacionais como a NATO e a OSCE, compreende-se que o panorama jurídico-político nacional em matéria de cibersegurança esteja alinhado com as medidas adotadas e compromissos assumidos no âmbito destas organizações (Lourenço, 2021, p. 23).

A primeira iniciativa no âmbito da cibersegurança ocorreu em 2009, com a aprovação da Lei n.º 109, de 15 de setembro, do Cibercrime, que tem como principal finalidade aumentar a segurança dos cidadãos no ciberespaço e conferir ferramentas de intervenção às entidades que combatem o cibercrime (Carballo-Cruz, 2022, p. 49).

Em 2011, o Ministério da Defesa Nacional aprovou o Decreto-Lei n.º 62/2011, de 9 de maio, o qual estabelece os procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social nos setores da energia e transportes (Carballo-Cruz, 2022, p. 49).

Por forma a implementar e consolidar uma Estratégia Nacional de Segurança da Informação, o governo português criou, em 2012, o Centro Nacional de Cibersegurança (CNCS), através da Resolução do Conselho de Ministros n.º 12/2012, de 7 de fevereiro, sendo as suas características, competências e regime de funcionamento definidos posteriormente, em 2014 (Carballo-Cruz, 2022, p. 49).

Em 2013, o governo estabeleceu um conjunto de prioridades no âmbito da proteção contra o Cibercrime e o Ciberterrorismo, sendo elas: a) garantir a proteção das infraestruturas de informação críticas; b) definir uma Estratégia Nacional de Cibersegurança; c) criar uma estrutura responsável pela Cibersegurança; d) sensibilizar os operadores sobre o carácter crítico da segurança da informação; e e) aumentar a capacidade de ciberdefesa (Carballo-Cruz, 2022, p. 49). A Estratégia Nacional de Segurança do Ciberespaço foi aprovada em 2015, através da Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, com o intuito de estabelecer objetivos e linhas de ação para melhorar a gestão das crises, a coordenação das respostas aos ciberataques, o

desenvolvimento de sinergias nacionais e a cooperação a nível nacional, internacional e europeu (ibidem, 2022, p. 49).

Inserida na estrutura orgânica da Polícia Judiciária, foi criada, em 2016, a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), em substituição da Unidade Nacional da Investigação da Criminalidade Informática, tendo como principal finalidade a prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias relativamente aos crimes praticados com recurso ou por meio de tecnologias (n.º 1 do artigo 9º do Decreto-Lei n.º 81/2016, de 28 de novembro).

Posteriormente, em 2018, foi aprovado, o Regime Jurídico da Segurança no Ciberespaço, através da Lei n.º 46/2018, de 13 de agosto, a qual prevê: a) a definição de uma nova Estratégia Nacional de Segurança do Ciberespaço, adaptada às necessidades impostas pela evolução das ameaças cibernéticas e dos riscos associados; b) a consagração do Centro Nacional de Cibersegurança como ponto de contacto único e Autoridade Nacional de Cibersegurança; C) a definição dos protocolos de segurança TIC, bem como dos requisitos e medidas de segurança das redes e sistemas de informação; e d) a definição das obrigações e procedimentos de notificação de incidentes, incluindo o regime sancionatório (Carballo-Cruz, 2022, p. 50).

Importa referir que o Regime Jurídico da Segurança no Ciberespaço é regulamentado através do Decreto-Lei n.º 65/2021, de 30 de julho, o qual estabelece: a) os requisitos de segurança das redes e dos sistemas de informação que devem ser cumpridos pela Administração Pública, pelos operadores de infraestruturas críticas e pelos operadores de serviços essenciais; e b) os requisitos de notificação de incidentes que afetem a segurança das redes e dos sistemas de informação que devem ser cumpridos pela Administração Pública, pelos operadores de infraestruturas críticas, pelos operadores de serviços essenciais e pelos prestadores de serviços digitais (n.º 2 do artigo 1º do Decreto-Lei n.º 65/2021, de 30 de julho). Além disso, o presente Decreto-Lei consagra as obrigações no que respeita à certificação da cibersegurança (Carballo-Cruz, 2022, p. 50).

A nova Estratégia Nacional de Segurança do Ciberespaço, em vigor para o período 2019-2023, foi promulgada através da Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho, estabelecendo como principais objetivos estratégicos: a) estruturar a segurança do ciberespaço; b) prever, educar e sensibilizar em matéria de cibersegurança; c) proteger o ciberespaço e as infraestruturas críticas; d) melhorar a resposta às ameaças e combater o cibercrime; e) apoiar a

investigação, o desenvolvimento e a inovação; e f) fomentar a cooperação nacional e internacional (Carballo-Cruz, 2022, p. 50).

Ainda em 2019, o Centro Nacional de Cibersegurança publicou o Quadro Nacional de Referência para a Cibersegurança (QNRCS), que integra um conjunto de medidas para lidar com os principais problemas no âmbito da cibersegurança (Carballo-Cruz, 2022, p. 50). Além desta iniciativa, destaca-se também o CERT.PT, integrado igualmente no CNCS, o qual coordena a resposta a incidentes que envolvam entidades da Administração Pública, operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais, assim como a totalidade do ciberespaço nacional (ibidem, 2022, p. 50). Adicionalmente, existe a Rede Nacional de CSIRT (RNCSIRT), constituindo-se como um fórum de partilha de informação de carácter operacional, cujos principais objetivos assentam em: a) promover um ambiente de cooperação entre os responsáveis pela segurança cibernética; b) desenvolver indicadores e informação estatística sobre incidentes cibernéticos; c) estabelecer instrumentos de prevenção e resposta rápida perante incidentes de grande dimensão; e d) promover uma cultura de segurança em Portugal (ibidem, 2022, p. 50).

Mais recentemente, em 2022, foram aprovadas as seguintes situações:

- Procedimentos para identificação, designação, proteção e aumento da resiliência das infraestruturas críticas nacionais e europeias (Decreto-Lei n.º 20/2022, de 28 de janeiro);
- Instrução técnica relativa às comunicações entre as entidades e o Centro Nacional de Cibersegurança (Regulamento n.º 183/2022, de 21 de fevereiro);
- Designação do Centro Nacional de Cibersegurança como centro nacional de coordenação para efeitos do Regulamento (EU) 2021/887 do Parlamento Europeu e do Conselho, de 20 de maio de 2021, e criação de consórcio entre o Centro Nacional de Cibersegurança, a Agência Nacional de Inovação e a Fundação para a Ciência e a Tecnologia (Despacho n.º 11491/2022, de 28 de setembro);
- Estratégia Nacional de Ciberdefesa (Resolução do Conselho de Ministros n.º 106/2022, de 2 de novembro).

De seguida, apresenta-se a Tabela 6, que resume o enquadramento legal da Cibersegurança explorado anteriormente.

Tabela 6: Enquadramento legal da Cibersegurança

Designação	Ano	Entidade responsável	Âmbito	Sumário
Diretiva 2002/58/CE	2002	Parlamento Europeu e Conselho da União Europeia	União Europeia	Estabelece as regras relativas ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas.
Diretiva 2008/114/CE	2008	Conselho da União Europeia	União Europeia	Estabelece um procedimento de identificação e designação das Infra-estruturas Críticas Europeias (ICE) e uma abordagem comum relativa à avaliação da necessidade de melhorar a sua proteção, de modo a contribuir para a proteção das pessoas.
Lei do Cibercrime	2009	Assembleia da República	Portugal	Estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico.
Decreto-Lei n.º 62/2011	2011	Ministério da Defesa Nacional	Portugal	Estabelece os procedimentos de identificação e de proteção das infra-estruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos sectores da energia e transportes.
Resolução do Conselho de Ministros n.º 12/2012	2012	Presidência do Conselho de Ministros	Portugal	Aprova o plano global estratégico de racionalização e redução de custos com as TIC na Administração Pública, apresentado pelo Grupo de Projeto para as Tecnologias de Informação e Comunicação (GPTIC).
Regulamento (UE) 2014/910	2014	Parlamento Europeu e Conselho da União Europeia	União Europeia	Estabelece as regras relativas à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno.
Resolução do Conselho de Ministros n.º 36/2015	2015	Presidência do Conselho de Ministros	Portugal	Aprova a Estratégia Nacional de Segurança do Ciberespaço.
Regulamento (UE) 2016/679	2016	Parlamento Europeu e Conselho da União Europeia	União Europeia	Estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Diretiva (UE) 2016/1148	2016	Parlamento Europeu e Conselho da União Europeia	União Europeia	Estabelece medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação na União, a fim de melhorar o funcionamento do mercado interno.
Decreto-Lei n.º 81/2016	2016	Justiça	Portugal	Cria a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica.
Lei n.º 46/2018	2018	Assembleia da República	Portugal	Estabelece o Regime Jurídico da Segurança do Ciberespaço.
Regulamento (UE) 2019/881	2019	Parlamento Europeu e Conselho da União Europeia	União Europeia	Estabelece os objetivos, as atribuições e os aspetos organizativos da ENISA, bem como um enquadramento para a criação de sistemas europeus de certificação da cibersegurança.
Resolução do Conselho de Ministros n.º 92/2019	2019	Presidência do Conselho de Ministros	Portugal	Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023.
Decreto-Lei n.º 65/2021	2021	Presidência do Conselho de Ministros	Portugal	Regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança.
Decreto-Lei n.º 20/2022	2022	Presidência do Conselho de Ministros	Portugal	Aprova os procedimentos para identificação, designação, proteção e aumento da resiliência das infraestruturas críticas nacionais e europeias.
Regulamento n.º 183/2022	2022	Presidência do Conselho de Ministros - Gabinete Nacional de Segurança - Centro Nacional de Cibersegurança	Portugal	Configura instrução técnica relativa a comunicações entre as entidades e o Centro Nacional de Cibersegurança.
Despacho n.º 11491/2022	2022	Presidência do Conselho de Ministros - Gabinetes do Ministro da Economia e do Mar, da Ministra da Ciência, Tecnologia e Ensino Superior e do Secretário de Estado da Digitalização e da Modernização	Portugal	Designação do Centro Nacional de Cibersegurança como centro nacional de coordenação e criação de consórcio entre o Centro Nacional de Cibersegurança, a Agência Nacional de Inovação, S. A., e a Fundação para a Ciência e a Tecnologia, I. P.

Resolução do Conselho de Ministros n.º 106/2022	2022	Presidência do Conselho de Ministros	Portugal	Aprova a Estratégia Nacional de Ciberdefesa.
Diretiva (UE) 2022/2555	2022	Parlamento Europeu e Conselho da União Europeia	União Europeia	Estabelece as medidas destinadas a garantir um elevado nível comum de cibersegurança na União, alterando o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revogando a Diretiva (UE) 2016/1148 (Diretiva SRI 2).

1.4. O papel do Estado

No âmbito do seu carácter regulador, legislador, executivo e securitário, o Estado enfrenta atualmente o desafio de tornar o ciberespaço um local seguro para as atividades dos seus cidadãos e empresas, contribuindo para o desenvolvimento de uma relação de confiança na utilização dos serviços cibernéticos por parte do setor público e privado (Lourenço, 2021, p. 12). Esta intervenção do Estado em matéria de cibersegurança deve fundamentar-se na elaboração de políticas públicas adequadas e da monitorização dos seus efeitos (ibidem, 2021, p. 12). A título exemplificativo, destacam-se, entre outras, a Estratégia Nacional de Segurança do Ciberespaço 2019-2023 e a Iniciativa Nacional de Competências Digitais e.2030 (INCoDe.2030) como políticas públicas desenvolvidas no caso específico do contexto português (ibidem, 2021, p. 29).

Segundo Asllani *et al.* (2013), os governos devem fornecer um quadro legal, social, ético, regulamentar e de responsabilidade abrangente para proteger indivíduos e organizações da ameaça do cibercrime (p. 10). Posto isto, devem ter um papel fundamental, através de iniciativas como: a) reforçar a educação pública sobre cibersegurança, através de incentivos que se concentrem na prevenção do cibercrime; b) melhorar o sistema de justiça criminal para combater o cibercrime, introduzindo e aprovando novas leis; c) combater e perseguir o ciberterrorismo, através da coordenação com agências que que promovam a segurança cibernética e o comportamento *online* seguro; d) fazer cumprir a regulamentação para a segurança da informação, impondo a conformidade regulamentar e a potencial responsabilidade em situação de violação da segurança; e) regulamentar os aspetos jurídicos, sociais e éticos da *Internet*, equilibrando os benefícios da tecnologia com a segurança e os direitos de liberdade; e f) proteger os direitos digitais, patentes, direitos de autor e leis de marcas registadas na *Internet* (ibidem, 2013, pp. 11-12). Contudo, numa abordagem inter-relacional entre governos e empresas, a possibilidade de os governos criarem uma garantia completa de cibersegurança é remota, pelo que é aconselhável uma abordagem mista, em

que o governo fornece o nível básico de segurança, enquanto as empresas podem diferenciar-se ao nível da sua segurança interna (ibidem, 2013, p. 13).

Por sua vez, Srinivas *et al.* (2018) acreditam que as instituições governamentais devem definir uma estratégia nacional de cibersegurança cujas prioridades passam por: a) desenvolver um sistema nacional de resposta à segurança do ciberespaço, que permita melhorar a resposta do governo perante ciberataques e reduzir potenciais danos resultantes de tais incidentes; b) desenvolver um programa de redução de ameaças e vulnerabilidades de segurança no ciberespaço; c) desenvolver um programa nacional de sensibilização e formação em matéria de cibersegurança; d) garantir uma maior intervenção do governo em questões de segurança cibernética; e e) estabelecer um sistema de segurança nacional e de cooperação internacional de segurança cibernética, não só para prevenir incidentes que possam ter impacto nos bens de segurança nacional, como também para melhorar a gestão e resposta internacional a ciberataques (p. 8).

No sentido de auxiliar a definir práticas eficazes para verificação da segurança nos sistemas nacionais relevantes e a normalizar os processos e aplicação dos regulamentos, Srinivas *et al.* (2018) apresentam um conjunto de recomendações úteis tanto para a segurança como para a defesa cibernética, nomeadamente: a) os decisores políticos devem encorajar não só os comerciantes a concordarem na utilização das normas, como também as organizações dos setores público e privado a incluir as referências das normas nos procedimentos de aquisição; b) os governos devem integrar a normatização como parte da sua política nacional de cibersegurança; c) as autoridades reguladoras nacionais devem utilizar uma maior aplicação das normas como ponto de referência, a fim de impor regulamentos; d) as organizações envolvidas no financiamento da investigação precisam de identificar conjuntos de normas compatíveis a serem utilizados em várias atividades de investigação, pelo que se revela necessário que a investigação financiada com fundos públicos cumpra as normas estabelecidas; e) a Organização de Desenvolvimento de Normas (SDO) necessita de trabalhar em conjunto para retificar várias formas de acelerar o processo de desenvolvimento de normas relacionadas com a segurança cibernética; e f) os governos dos países cooperantes devem definir um amplo esquema de certificação que permita aos utilizadores verificar se os produtos ou serviços dos quais dependem obedecem a normas de segurança (p. 10).

Embora o Estado assuma um papel determinante na política de segurança cibernética, Cavelty e Egloff (2019) sublinham que a cibersegurança revela-se como uma questão transversal típica, que requer a cooperação entre uma grande variedade de atores, sendo eles autoridades públicas, mas também empresas e a própria sociedade (p. 48). A verdade é que muitas redes cruciais estão sob alçada de entidades privadas, pelo que o Estado por si só não consegue garantir

a sua proteção contra ciberataques (ibidem, 2019, p. 49). Não obstante, o Estado constituiu-se como um dos principais atores e, por esse motivo, atua como protetor das suas próprias redes civis e militares contra qualquer forma de conflito cibernético (ibidem, 2019, p. 49). Ao nível da sua função de legislador e regulador, o Estado desenvolve a base jurídica necessária para clarificar a sua função hierárquica perante a sociedade e a economia no que toca à cibersegurança, bem como constitui um quadro jurídico para regular a tensão entre os cidadãos e as empresas (ibidem, 2019, p. 49). Dado que os atores no ciberespaço operam frequentemente a nível internacional, as instituições estatais atuam também como representantes da sociedade, defendendo quadros internacionais que são conducentes tanto à respetiva economia como à sociedade, assumindo, muitas vezes, o papel de parceiros (ibidem, 2019, p. 49). Por último, o Estado desempenha frequentemente o papel de criador e divulgador de conhecimento, sendo visto como uma fonte de informação fidedigna (ibidem, 2019, p. 49).

No conjunto de papéis que deve desempenhar, Kelly (2023) defende que o Governo deve, primeiramente, contratar uma Agência Nacional de Cibersegurança, com o intuito de desenvolver uma estratégia nacional de segurança cibernética alinhada com um conjunto de iniciativas que pretendem proteger a infraestrutura crítica, mobilizar a resposta a crimes e definir padrões de segurança cibernética que ofereçam proteção máxima em todas as entidades governamentais. Por forma a evitar que ocorram ameaças à infraestrutura crítica do país, o Governo deve construir um Programa Nacional de Proteção de Infraestrutura Crítica, procurando trabalhar com cada setor para compreender as suas ameaças e a segurança necessária para protegê-los (ibidem, 2023). Adicionalmente, o Governo deve criar um Plano Nacional de Resposta a Incidentes, no sentido de mitigar os efeitos de incidentes cibernéticos e melhorar seu o tempo de recuperação (ibidem, 2023). Por último, os organismos governamentais devem definir leis relacionadas com ciberataques (ibidem, 2023).

1.5. Entidades com autoridade em matéria de Cibersegurança

Para uma melhor gestão de questões relacionadas com a ocorrência de ciberataques, é fundamental a definição de entidades com autoridade para coordenar a avaliação e resposta a incidentes cibernéticos.

Do ponto de vista institucional, Portugal integra um conjunto de entidades com autoridade em matéria de Cibersegurança, sendo elas (Andrade *et al.*, 2020, pp. 48-53):

Tabela 7: Entidades portuguesas com autoridade em matéria de Cibersegurança

Entidade	Principais responsabilidades
Gabinete Nacional de Segurança (GNS)	Serviço central da administração direta do Estado, dotado de autonomia administrativa, na dependência do Primeiro-Ministro. Tem por missão garantir a segurança da informação classificada no âmbito nacional e das organizações internacionais de que Portugal é membro, bem como exercer a função de autoridade de credenciação de pessoas singulares ou coletivas para o acesso e manuseamento de informação classificada, de autoridade credenciadora e de fiscalização de entidades.
Centro Nacional de Cibersegurança (CNCS)	Organismo que funciona no âmbito do Gabinete Nacional de Segurança. Tem por missão contribuir para que Portugal utilize o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da definição e implementação das medidas e instrumentos necessários à antecipação, deteção, reação e recuperação de situações que ponham em causa o interesse nacional.
Conselho Superior de Segurança do Ciberespaço	Criado, em 2017, na sequência da aprovação da primeira Estratégia Nacional de Segurança do Ciberespaço de 2015, para funcionar como "grupo de projeto", na dependência do Primeiro-Ministro, com a missão de assegurar a coordenação político-estratégica para a segurança do ciberespaço e o controlo da execução da Estratégia Nacional e respetiva revisão.
Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária (UNC3T)	Unidade operacional especializada da Polícia Judiciária (PJ), inspirada no modelo adotado pelo EC3 da Europol. Tem como principal competência a prevenção, deteção e investigação dos crimes previstos na Lei do Cibercrime, bem como dos crimes praticados com recurso ou por meio de tecnologias ou de meios informáticos.
Gabinete de Coordenação da Atividade do Ministério Público na Área da Cibercriminalidade	O Gabinete Cibercrime funciona na direta dependência da Procuradoria-Geral da República. Tem como missão a coordenação interna do Ministério Público na área da cibercriminalidade, a formação específica de Magistrados do Ministério Público nesta matéria, a interação com o setor privado, através do estabelecimento de canais de comunicação com fornecedores de serviço de acesso às redes de comunicação para fins de facilitação da sua colaboração na investigação criminal, a interação com os órgãos de polícia criminal e, residualmente, o acompanhamento de processos concretos.
Equipa de Resposta a Incidentes de Segurança Informática Nacional (CERT.PT)	Serviço integrante do CNCS que coordena a resposta a incidentes ocorridos no ciberespaço nacional envolvendo entidades do Estado, operadores de serviços essenciais, operadores de infraestruturas críticas nacionais e prestadores de serviços digitais.
Comissão Nacional de Proteção de Dados (CNPD)	Entidade administrativa independente, com poderes de autoridade, que funciona junto da Assembleia da República. Tem como atribuição genérica controlar e fiscalizar o cumprimento do Regulamento Geral de Proteção de Dados (RGPD) e da Lei n.º 58/2019, bem como das demais disposições legais e regulamentares que versem sobre a proteção de dados pessoais, com o fim de defender os direitos, liberdades e garantias das pessoas singulares no âmbito do tratamento de dados pessoais.

À semelhança do quadro legal, estas entidades colaboram estreitamente com as entidades europeias – o CNCS trabalha em articulação com a ENISA, o CERT.PT com a Rede Europeia de CSIRT57, e a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária (UNC3T) com o Centro Europeu de Cibercriminalidade (EC3) da Europol (Carballo-Cruz, 2022, p. 51).

A nível de entidades internacionais, o *Cybersecurity: A Generic Reference Curriculum* aponta, com especial destaque, a Agência Europeia para a Segurança das Redes e da Informação (ENISA), a Organização para a Segurança e Cooperação na Europa (OSCE), as Nações Unidas e a NATO (NATO, 2016, p. 42). Importa mencionar, também, algumas agências, como sendo o *Global Forum for Incident Response and Security Teams*, a *International Multilateral Partnership Against Cyber Threats* (IMPACT) e a *Armed Forces Communications and Electronics Association* (AFCEA) (ibidem, 2016, p. 42). Entre outros organismos internacionais preocupados com a Cibersegurança, destacam-se a Organização Internacional de Normalização, a Corporação da Internet para Atribuição de Nomes e Números (ICANN), o Fórum de Governação da Internet (IGF) e a União Internacional de Telecomunicações (UIT) integrada na ONU (ibidem, 2016, p. 42).

1.6. A importância da Cibersegurança

Durante as primeiras décadas da sua existência, as redes de computadores eram utilizadas principalmente por investigadores universitários para enviar *e-mails* e por colaboradores de algumas empresas, que as utilizavam para partilhar impressoras, não sendo, por esse motivo, uma grande preocupação (Tanenbaum & Wetherall, 2011, p. 763). Contudo, atualmente existem milhões de utilizadores que as estão a utilizar para realizar operações bancárias, fazer compras, apresentar as suas declarações de impostos, resultando em inúmeras vulnerabilidades, pelo que a cibersegurança começou a assumir uma maior magnitude (ibidem, 2011, p. 763). A cibersegurança é agora considerada como parte integrante da vida de indivíduos, organizações e governos, embora a rápida expansão das tecnologias esteja a torná-la mais desafiante, devido à falta de soluções permanentes para problemas preocupantes (Goutam, 2015, p. 14).

A verdade é que os ciberataques têm um grande impacto na sociedade, provocando danos em diversas dimensões, nomeadamente (Agrafiotis *et al.*, 2018, pp. 7-10):

a) Dimensão digital ou física, traduzindo-se num efeito negativo de carácter digital ou físico sobre algo ou alguém, como sendo a destruição, indisponibilidade, roubo ou comprometimento do bem afetado;

b) Dimensão económica, traduzindo-se em danos relacionados com prejuízos financeiros ou consequências económicas, tais como redução de vendas ou volume de negócios, redução de clientes, redução de lucros, queda no preço das ações ou redução de capital;
c) Dimensão psicológica, que consiste em danos que se centram num indivíduo e no seu bem-estar mental, provocando sentimentos negativos como confusão, desconforto, ansiedade, vergonha, culpa ou insatisfação;
d) Dimensão reputacional, em que os danos resultam na perceção pública danificada, na relação prejudicada com clientes e fornecedores, na redução das oportunidades de negócio, na incapacidade de recrutar o pessoal desejado, no escrutínio por parte dos *media* ou na perda de colaboradores-chave;
e) Dimensão social, em que os danos podem ter influência num contexto social ou sociedade mais ampla, através de mudanças negativas na perceção pública, impacto nas atividades quotidianas ou redução da cultura organizacional interna.

Entre as principais razões para a ocorrência de ciberataques, Aslan *et al.* (2023) destacam a estrutura dos sistemas informáticos e das redes de comunicação, ou seja, as vulnerabilidades, deficiências e configurações erradas de *hardware*, *software* e redes informáticas expõem os sistemas a ataques explorados por *hackers* (pp. 10-11). Com o rápido desenvolvimento da tecnologia, novos dispositivos e *software* estão a ser adicionados diariamente ao ambiente da *Internet*, nomeadamente *smartphones*, *tablets*, dispositivos IoT e tecnologia *cloud*, sendo esta outra razão para o aumento do número de ataques informáticos (ibidem, 2023, p. 12). De destacar, também, o aumento do conhecimento como uma das principais razões desta tendência, uma vez que, nos últimos anos, tornou-se mais fácil iniciar ataques informáticos devido à utilização generalizada de ferramentas de ataque, à rápida disseminação de conhecimentos e à fácil deteção de vulnerabilidades em *software* informático e protocolos de rede, o que significa que, atualmente, qualquer pessoa pode tornar-se um *hacker* (ibidem, 2023, p. 14). Outra das razões prende-se com o facto de, nos últimos anos, se ter assistido a uma transferência da vida quotidiana para um ambiente digital, desde a própria socialização à realização de negócios *online* (ibidem, 2023, p. 15). Por último, importa mencionar que a facilidade de ataque à *Internet*, a ausência de fronteiras geográficas e a escassa legislação existente entre países no que diz respeito à punição dos cibercriminosos podem ser igualmente citadas como razões para o aumento dos ciberataques (ibidem, 2023, p. 15).

Chen (2023) defende que a cibersegurança é de extrema importância tanto para os consumidores como para as próprias organizações (p. 47). Enquanto os consumidores querem sentir que os dados que fornecem às organizações estão seguros, as organizações estão cada vez

mais preocupadas em garantir a segurança dos dados pessoais dos seus clientes e a confidencialidade de informações organizacionais (ibidem, 2023, p. 47). Embora estes obstáculos sejam extremamente difíceis de ultrapassar, podem ser evitados com a implementação de medidas rigorosas de cibersegurança (ibidem, 2023, p. 47).

A verdade é que os ciberataques podem prejudicar a reputação de uma organização, fazendo com que muitos clientes a abandonem, o que resulta numa perda significativa de vendas (Chen, 2023, p. 52). Por esse motivo, revela-se necessário que as organizações estejam bem preparadas antes da ocorrência de um ciberataque, por forma a saberem como gerir eficazmente a ameaça quando esta ocorrer (ibidem, 2023, p. 55). A formação e a educação dos colaboradores sobre cibersegurança e a sua importância poderão contribuir para uma maior sensibilização no que respeita a esta questão (ibidem, 2023, p. 55).

1.7. Vulnerabilidades e ataques informáticos

1.7.1. Tipologia dos ataques informáticos

Atualmente, assiste-se a um conjunto de diferentes tipos de ataque a emergir na *Internet*, descritos na Tabela 8.

Tabela 8: Principais problemas de segurança prevalecentes na *Internet* (adaptado de Comer, 2015)

Problema	**Descrição**
Phishing	Falsificação de um *site* conhecido, para obter informações pessoais dos utilizadores, normalmente uma *password* ou um número de conta bancária
Deturpação	Fazer afirmações falsas ou exageradas de bens ou serviços, assim como simular vendas ou vender produtos de qualidade inferior ao descrito
Fraude	Enganar utilizadores ingénuos a investir dinheiro ou a ser cúmplices de um crime
Negação de serviço	Bloquear intencionalmente um determinado *site* da *Internet* para impedir ou dificultar o seu normal funcionamento
Perda de controlo	Obter o controlo do computador de um utilizador e utilizá-lo para cometer um crime
Perda de dados	Perder propriedade intelectual ou outra informação comercial de propriedade valiosa

Embora Comer (2015) não tenha considerado os seguintes problemas, importa considerá-los também como ataques prevalecentes na *Internet*.

- ***Zero-day Exploit***

Consiste num ataque que explora uma vulnerabilidade anteriormente desconhecida, partindo do pressuposto de que os ataques acontecem no "dia zero" da tomada de consciência desta vulnerabilidade e, portanto, os *hackers* podem explorá-la livremente antes desta ser mitigada (Singer & Friedman, 2014, p. 42).

- ***Malware***

Sendo o resultado da conjugação entre as palavras "*malicious*" e "*software*", esta técnica consiste em danificar, perturbar, roubar ou infligir alguma ação ilegítima ou não autorizada num sistema ou rede de dados (Goodman, 2015, p. 17). Pode assumir diferentes tipos, nomeadamente:

  - ***Ransomware***: Restringe o acesso a um alvo e exige pagamento para devolver um serviço regular (Singer & Friedman, 2014, p. 298);

  - **Vírus**: Programa que se pode replicar e propagar de computador para computador (Singer & Friedman, 2014, p. 299);

  - ***Worm***: Espalha-se automaticamente por uma rede, instalando-se e replicando-se a si próprio (Singer & Friedman, 2014, p. 299). O tráfego de rede de rápida replicação e propagação pode danificar as redes, mesmo quando o *malware* não tem uma carga útil maliciosa (ibidem, 2014, p. 299);

  - ***Trojan***: Tipo de *malware* disfarçado ou ligado a um *software* legítimo ou inocente, mas que em vez disso transporta uma carga útil maliciosa, permitindo a entrada a utilizadores não autorizados (Singer & Friedman, 2014, p. 299);

  - ***Adware***: Utilizado para publicidade forçada, redirecionando o utilizador para alguma página de publicidade ou *pop-up* de uma página adicional que promove algum produto ou evento (Pande, 2017, p. 19);

  - ***Spyware***: É instalado no computador de destino com o propósito de roubar informações pessoais ou confidenciais do utilizador (Pande, 2017, p. 19). Na maioria das vezes, recolhe os hábitos de navegação do utilizador e envia-os para o servidor remoto sem o seu conhecimento (ibidem, 2017, p. 19);

  - ***Browser hijacking software***: Tipo de *malware* que é descarregado juntamente com o *software* gratuito disponibilizado através da *Internet* e instalado no computador sem o

conhecimento do utilizador (Pande, 2017, p. 19). Este *software* modifica a configuração dos *browsers* e redireciona as ligações para outros *sites* não intencionais (ibidem, 2017, p. 19).

1.7.2. Tecnologia de ataque

Habitualmente, os *hackers* utilizam técnicas específicas de ataque informático, as quais se encontram enumeradas na Tabela 9.

Tabela 9: Principais técnicas utilizadas em ataques de cibersegurança (adaptado de Comer, 2015)

Técnica	**Descrição**
Wiretapping	Fazer uma cópia dos pacotes à medida que atravessam uma rede, por forma a obter informações
Replay	Enviar pacotes capturados de uma sessão anterior (ex.: um pacote de *password* a partir de um *login* anterior)
Buffer Overflow	Enviar mais dados do que o recetor espera, com o intuito de armazenar os valores das variáveis para além do *buffer*
Address Spoofing	Falsificar o endereço de origem num pacote, para enganar o recetor no processamento dos pacotes
Name Spoofing	Utilizar nomes de domínios conhecidos, com apenas um erro de ortografia e com ligações incorretas
DoS (*Denial of Service*) e DDoS (*Distributed Denial of Service*)	Sobrecarregar um *site* com pacotes para impedir o seu normal funcionamento
SYN Flood	Enviar um fluxo aleatório de pacotes SYN, para esgotar o conjunto de ligações TPC de um recetor
Password Breaking	Adivinhar automaticamente uma *password* ou uma chave cripto para aceder a dados não autorizados
Port Scanning	Tentar conectar-se a cada porta de protocolo possível num *host*, para encontrar uma vulnerabilidade
Packet Interception	Remover um pacote da *Internet*, permitindo substituí-lo e efetuar ataques *man-in-the-middle*

1.7.3. Tecnologia de defesa

Por forma a mitigar as perturbações causadas pelos *hackers*, tem-se vindo a desenvolver um conjunto de técnicas de segurança que desempenham uma variedade de funções (Comer, 2015, p. 547). A Tabela 10 resume as principais técnicas utilizadas para aplicar políticas de segurança.

Tabela 10: Principais técnicas utilizadas para aplicar políticas de segurança (adaptado de Comer, 2015)

Técnica	**Propósito**	**Descrição**
Hashing	Integridade dos dados	Consiste em fornecer um código de autenticação de mensagens que depende de uma chave secreta conhecida apenas pelo emissor e pelo recetor e que um *hacker* não consegue falsificar
Encriptação	Privacidade	Consiste em codificar os *bits* de uma mensagem de tal forma que só o destinatário os pode descodificar, sendo que se alguém efetuar uma cópia dessa mensagem não conseguirá extrair informação
Assinaturas Digitais	Autenticação de mensagens	Consiste em encriptar uma mensagem utilizando uma chave conhecida apenas pelo emissor, sendo que o destinatário utiliza a função inversa para decifrar a mensagem
Certificados Digitais	Autenticação do emissor	Conhecendo uma chave - a chave pública de uma chave de autoridade -, consiste em obter um conjunto de chaves públicas de forma segura, fazendo com que o administrador só tenha de configurar uma delas
Firewalls	Integridade do *site*	Consiste numa tecnologia que ajuda a proteger os computadores e redes de uma organização de todo o tráfego indesejado da *Internet*, sendo colocada entre a organização e o resto da *Internet*, por forma a garantir que todos os pacotes que entram ou saem da organização passem através dela
Intrusion Detection Systems (IDS)	Integridade do *site*	Consiste em monitorizar todos os pacotes que chegam a um *site* e notificar o seu administrador caso sejam detetadas violações de segurança
Content Analysis	Integridade do *site*	Consiste numa técnica criada com o intuito de evitar problemas como a instalação de um vírus
Virtual Private Networks (VPNs)	Confidencialidade dos dados	Consiste numa das tecnologias de segurança mais importantes e amplamente utilizadas, recorrendo à encriptação para fornecer um acesso seguro à *intranet* de uma organização a partir de um local remoto

1.8. Casos de ciberataque a nível nacional e internacional

Em consequência do aumento significativo do número de ciberataques desde 2020, revelou-se pertinente fazer uma investigação exploratória que comprove esta tendência a nível nacional, fundamentada na crescente cobertura de incidentes por parte dos *media* portugueses. Adicionalmente, por forma a comprovar que estamos perante um crescimento que acompanha a

tendência internacional, apresentam-se alguns casos de ciberataques internacionais que decorreram igualmente nos últimos três anos e com expressão no domínio público nacional.

- **Nacional**

Tabela 11: Cronologia de ciberataques em Portugal

Data	Empresa
13 de abril de 2020	EDP
16 de abril de 2020	Altice Portugal
2 de janeiro de 2022	Grupo Impresa
8 de fevereiro de 2022	Vodafone Portugal
10 de fevereiro de 2022	Grupo Germano de Sousa
30 de março de 2022	Grupo Sonae
26 de abril de 2022	Hospital Garcia de Orta
14 e 25 de maio de 2022	Agência Lusa
Agosto de 2022	Estado-Maior-General das Forças Armadas
25 de agosto de 2022	TAP Air Portugal
15 de setembro de 2022	Sporting Clube de Portugal
15 de setembro de 2022	Futebol Clube do Porto
22 de setembro de 2022	Câmara Municipal de Loures
3 de outubro de 2022	Millennium BCP
18 de novembro de 2022	Segurança Social
19 de novembro de 2022	Câmara Municipal de Faro
30 de novembro de 2022	Universidade Católica Portuguesa
6 a 8 de dezembro de 2022	PayPal
15 de dezembro de 2022	INEM
28 de janeiro de 2023	Direção-Geral da Saúde
28 de janeiro de 2023	Faculdade de Farmácia da Universidade de Lisboa
30 de janeiro de 2023	Grupo Super Bock
8 de fevereiro de 2023	Global Media Group
13 de fevereiro de 2023	Grupo Visabeira
6 de abril de 2023	Ministério da Economia

7 de junho de 2023	Grupo Luís Simões
6 de agosto de 2023	Serviço de Saúde da Madeira

Durante o ano de 2020, decorreram em Portugal dois grandes incidentes cibernéticos que marcaram a agenda mediática. No dia 13 de abril, a EDP foi alvo de um ataque informático que teve implicações no normal funcionamento de uma parte dos serviços e operações da empresa, embora o fornecimento de energia não tenha sofrido qualquer impacto (Diário de Notícias, 2020). Três dias mais tarde, a 16 de abril, a Altice Portugal confirmou o ataque informático de que foi alvo, garantindo que "as consequências deste foram praticamente nulas" (Lusa, 2020).

A partir de 2022, o número de empresas a sofrer violações de segurança começou a aumentar gradualmente, sendo o Grupo Impresa a primeira. No dia 2 janeiro, os *sites* do jornal Expresso e da SIC ficaram indisponíveis, revelando uma mensagem dos *hackers* nas suas páginas a informar que se tratava de um ataque *ransomware*, exigindo dinheiro em troca da recuperação do controlo dos *sites* (Machado *et al.*, 2022). Além disso, o mesmo grupo que provocou o ataque informático enviou uma SMS para os telemóveis dos subscritores da plataforma de *streaming* Opto, bem como um *e-mail* para os subscritores das *newsletters* do Expresso (ibidem, 2022).

Caracterizado pela sua magnitude, seguiu-se o ciberataque à Vodafone Portugal que, segundo Mário Vaz, CEO da empresa, "teve origem num ato terrorista e criminoso" (Miranda, 2022). Na madrugada do dia 8 de fevereiro de 2022, a Vodafone deparou-se com a indisponibilidade de praticamente todos os seus serviços de telecomunicações – serviço de voz, serviço de SMS, *internet* fixa, *internet* móvel, televisão –, afetando quatro milhões de clientes, embora não houvesse indícios de acesso aos seus dados pessoais (ibidem, 2022). De acordo com a perspetiva de José Tribolet, professor catedrático no Instituto Superior Técnico e presidente do INESC, "foi o primeiro ataque em Portugal de origem geopolítica e que visou invalidar uma estrutura fundamental do país, como tem havido muitos outros na NATO. É um ataque a uma empresa, mas é sobretudo um ataque à nação portuguesa" (Tribolet in Dias, 2022). A pertinência deste caso, em particular, deve-se à transparência da comunicação e gestão de crise elogiadas como boas práticas. Lino Santos, coordenador do CNCS, garante que "só posso deixar elogios" em relação à forma como a Vodafone comunicou a situação (Santos in Caçador, 2022b).

Posteriormente, na madrugada do dia 10 de fevereiro de 2022, os laboratórios Germano de Sousa foram igualmente alvo de um ataque informático, afetando apenas o sistema de registos – os dados dos pacientes foram salvaguardados (RTP, 2022). Embora o Grupo tenha conseguido assegurar os exames e garantir o trabalho dentro da normalidade possível, as ligações entre os

laboratórios e os hospitais ficaram suspensas, por forma a não comprometer os restantes serviços (ibidem, 2022).

No dia 30 de março de 2022, seguiu-se um ciberataque ao Grupo Sonae, que detém os hipermercados Continente, afetando algumas comunicações nos *sites* comerciais e alguns serviços em loja (Marques, 2022). Entre os serviços afetados, destaca-se o serviço *online* da marca de retalho alimentar do Continente, assim como o cartão Continente, ainda que as lojas físicas tenham mantido o seu normal funcionamento (ibidem, 2022).

Na madrugada de 26 de abril de 2022, foi a vez do Hospital Garcia de Orta sofrer um ciberataque, que provocou o cancelamento de consultas e cirurgias, bem como constrangimentos na realização de TACs e radiografias, estando o hospital sem acesso à rede (Évora *et al.*, 2022). Tratou-se de um ataque de *ransomware*, em que os *hackers* exigiram um valor, pago em *bitcoins*, para o hospital voltar a ter acessos aos dados (ibidem, 2022).

Também a Agência Lusa foi alvo de um ciberataque, no dia 14 de maio de 2022, seguindo-se um segundo ataque que ocorreu no dia 25 do mesmo mês (Lusa, 2022a). Ambos os incidentes causaram instabilidade na prestação de serviços da empresa, quer interna, quer externamente (ibidem, 2022a).

Durante o mês de agosto de 2022, decorreram dois ataques de grande magnitude a nível nacional. O primeiro visou o Estado-Maior-General das Forças Armadas, permitindo aos *hackers* o acesso a centenas de documentos secretos e confidenciais da NATO, que foram colocados à venda na *Dark Web* (Público, 2022). O segundo, com início no dia 25 de agosto, teve como alvo a companhia aérea TAP, expondo publicamente a informação privada de 1,5 milhões de passageiros na *Internet*, incluindo nomes, moradas e, inclusive, alegados acordos comerciais da empresa – confirmando-se ser um ataque *ransomware* (Nunes, 2022).

Também os *sites* do Sporting Clube de Portugal e do Futebol Clube do Porto foram afetados temporariamente na sequência de ataques informáticos, ambos do tipo DDoS (*Distributed Denial of Service*), tornando indisponível o acesso aos *sites* devido a um número excessivo de pedidos de acesso que sobrecarregaram o sistema (Diário de Notícias, 2022b).

Posteriormente, a Câmara Municipal de Loures anuncia que foi alvo de um ciberataque, na madrugada do dia 22 de setembro (Diário de Notícias, 2022a). Caracterizado como um "ciberataque malicioso e deliberado", a autarquia refere que o objetivo era provocar perturbações no sistema e serviços informáticos (ibidem, 2022). No mês de novembro, também a Câmara

Municipal de Faro sofreu um incidente de *ransomware* que afetou o normal funcionamento dos serviços (Costa, 2022).

No início de outubro de 2022, foi a vez do Millennium BCP sofrer um ataque informático, que impossibilitou o acesso dos clientes ao *site* e às aplicações para telemóveis (Neutel, 2022). Este ataque classifica-se como sendo DoS (*Denial of Service*) e, por norma, não inclui a vertente de acesso ilegal a dados internos da organização – tal como se confirmou no caso do BCP (ibidem, 2022).

Outro incidente com grande impacto à escala nacional foi o ciberataque à Segurança Social, que ocorreu durante o mês de novembro de 2022, tendo como principal objetivo a destruição das bases de dados (Séneca, 2022a). Mais tarde, veio a comprovar-se que, embora os dados dos contribuintes e empresas não tenham sido comprometidos, foram expostos os nomes de 14 mil trabalhadores da Segurança Social (Jornal de Notícias, 2023).

Por sua vez, a Universidade Católica Portuguesa e o INEM confirmaram ter sido alvos de ataques informáticos (Séneca, 2022b). Ainda no mês de novembro, o ciberataque ao Polo da Universidade Católica do Porto obrigou à suspensão de vários serviços disponibilizados a alunos e professores, tendo um impacto direto nas atividades letivas durantes duas semanas (ibidem, 2022b). No caso do INEM, o ciberataque poderá ter concedido acesso a senhas e outras credenciais de 2492 profissionais, bem como ter afetado alguns serviços, como sendo plataformas que suportam horários, que distribuem ferramentas de trabalho através da *Internet* ou que permitem alterar *passwords* (ibidem, 2022b). Ainda assim, a atividade de emergência médica não ficou comprometida, nem os dados dos próprios utentes (ibidem, 2022b).

Para terminar o ano de 2022, o PayPal anunciou que foi vítima de um ciberataque, que comprometeu a informação pessoal de mais de 35 mil utilizadores do serviço (Dias, 2023). Entre os dados roubados, encontram-se nomes, nomes de utilizador, endereços, datas de nascimento e, inclusive, números de Segurança Social (ibidem, 2023).

O ano de 2023 começou com o ataque informático ao *site* da Direção-Geral da Saúde, impedindo o acesso aos seus dados e serviços (Lusa, 2023a). O incidente surgiu por parte de um grupo de ciberativistas russos, afetando também o *site* da Faculdade de Farmácia da Universidade de Lisboa, embora os constrangimentos tenham sido rapidamente solucionados (ibidem, 2023a).

No final do mês de janeiro de 2023, seguiu-se o ciberataque ao Grupo Super Bock – que detém marcas como a Super Bock, Carlsberg, Somersby e Frutis –, provocando perturbações nos

seus serviços informáticos, além de constrangimentos nas operações de abastecimento de alguns dos seus produtos no mercado (Público, 2023).

A 8 de fevereiro de 2023, também a Global Media Group confirmou ter sido alvo de um ciberataque em alguns dos seus *sites*, embora, segundo informação do presidente, não tenha causado nenhum tipo de constrangimento nos órgãos de comunicação do grupo (Lusa, 2023c). O ciberataque foi liderado por um pirata informático português conhecido como "Zambrius", que atua no grupo denominado "Cyber Team" (ibidem, 2023c).

Ainda no mês de fevereiro, o Grupo Visabeira foi igualmente vítima de um ciberataque que provocou constrangimentos no normal funcionamento de um conjunto de serviços, os quais foram interrompidos pela própria empresa (Lusa, 2023d).

Seguiu-se o ataque informático ao Ministério da Economia, decorrido a 6 de abril de 2023, que afetou, de forma parcial, alguns *sites* de organismos tutelados pelo ministério (Lusa, 2023e). Contudo, até ao final do dia do incidente, o Ministério da Economia conseguiu restabelecer 85% do impacto causado pelo ciberataque, sem comprometimento de informação (ibidem, 2023e).

Durante o mês de junho, o Grupo Luís Simões confirmou ter sido vítima de um ataque informático, embora não tenha afetado os serviços de transporte e logística da empresa (Séneca, 2023). Não obstante, os *hackers* acederam a dados pessoais de colaboradores e clientes, ameaçando partilhá-los na *Dark Web* (ibidem, 2023).

Já em agosto de 2023, foi a vez do Serviço de Saúde da Madeira (SESARAM) sofrer um ciberataque que provocou uma "disfunção na sua rede informática", obrigando à suspensão da atividade clínica não urgente durante o dia seguinte – incluindo consultas, cirurgias programadas, análises clínicas e meios complementares de diagnóstico (Lusa, 2023f). Ao afetar o funcionamento interno do SESARAM, o ciberataque comprometeu várias áreas, nomeadamente o Serviço de Urgência do Hospital Dr. Nélio Mendonça, no Funchal, assim como provocou "constrangimentos nas ligações telefónicas" dos centros de saúde, levando à disponibilização de números de telefone provisórios (ibidem, 2023f).

- **Internacional**

A guerra entre a Rússia e a Ucrânia tem sido o grande palco de ciberataques a nível mundial nos últimos tempos. Segundo Ilya Vitiuk, chefe do departamento de cibersegurança no Serviço de Segurança da Ucrânia (in Lusa, 2022c), foram registados cerca de 800 ciberataques em 2020, mais de 1.400 em 2021 e mais de 4.500 em 2022 (ibidem, 2022c). De mencionar que os setores do

território ucraniano mais afetados pelos ataques russos dizem respeito à energia e logística, instalações militares e, ainda, bases de dados governamentais e fontes de informação (ibidem, 2022c).

Outro incidente cibernético de grande escala a nível mundial atingiu o Governo dos EUA, em dezembro de 2020 (Soares, 2020). Caracterizado como sendo um ataque "altamente complexo", sofisticado, sem precedentes e com riscos "graves" para os EUA e para todo o mundo, o incidente foi detetado, inicialmente, nos departamentos do Tesouro e do Comércio (ibidem, 2020). Contudo, o ataque afetou muitos mais níveis do governo norte-americano, nomeadamente as principais agências governamentais, desde o Departamento da Defesa, de Segurança Interna e, inclusive, a agência que supervisiona o arsenal de armas nucleares dos EUA, além de grandes empresas de tecnologia e segurança, incluindo a Microsoft (ibidem, 2020). O ataque concretizou-se através do envio de *malware*, possibilitando aos *hackers* o acesso remoto às redes para que pudessem roubar informações (ibidem, 2020).

No início de 2022, o Comité Internacional da Cruz Vermelha (ICRC), com sede em Genebra, na Suíça, informou que teria sido alvo de um ciberataque, resultando no comprometimento dos dados pessoais e confidenciais de mais de 515 mil "pessoas altamente vulneráveis" (Cipriano, 2022). O incidente causou perturbações nos sistemas informáticos associados a um programa que reúne famílias separadas pelo conflito, migração ou desastres, pessoas desaparecidas e os seus familiares, assim como pessoas detidas (ibidem, 2022).

Importa destacar, também, o ciberataque à Ronin Network, plataforma de validação do jogo Axie Infinity, que ocorreu a 23 de março de 2022 (Silva, 2022). O ataque envolveu o roubo de 625 milhões de dólares em *ethereum* e USDC, uma das mais destacadas *stablecoins* do mercado das criptomoedas, sendo considerado como o maior ataque alguma vez noticiado contra uma plataforma cripto (ibidem, 2022).

Posteriormente, foi a vez da Amnistia Internacional no Canadá ser vítima de um incidente cibernético por parte da China, afastando a organização da *Internet* durante quase três semanas (Lusa, 2022b).

Ainda em 2022, seguiu-se um ataque informático à empresa Meta, mais especificamente à sua rede social *WhatsApp* (Monteiro, 2022). A nível global, o ataque provocou a fuga de 360 milhões de números de telefone de utilizadores do *WhatsApp* de mais de uma centena de países (ibidem, 2022). No caso específico de Portugal, mais de 2,2 milhões de registos de utilizadores terão sido encontrados à venda na *Dark Web* (ibidem, 2022).

Mais recentemente, em fevereiro de 2023, o serviço de *Internet* em Itália foi igualmente alvo de um ataque informático "massivo", que provocou problemas informáticos (Lusa, 2023b). Além de Itália, o incidente afetou também outros países europeus e a América do Norte, sendo classificado como um ataque de *ransomware* (ibidem, 2023b).

1.9. Medidas de prevenção e defesa

À medida que as novas tecnologias se incorporam nas múltiplas atividades diárias, revela-se necessário investir e desenvolver em culturas de cibersegurança dentro das organizações, por forma a diminuir o risco do fator humano, conferir um impacto positivo na eficiência e segurança e atenuar os riscos financeiros da organização (ENISA, 2017, p. 7). Por cultura de cibersegurança de uma organização, entende-se o conjunto de conhecimento, crenças, perceções, atitudes, pressupostos, normas e valores das pessoas relativamente à cibersegurança e a forma como estes se manifestam nos seus comportamentos com as tecnologias de informação (ibidem, 2017, p. 7). Por se tratar de uma cultura, compreende-se que as preocupações inerentes à cibersegurança se constituam como parte integrante do trabalho, hábitos e conduta dos colaboradores, integrando o seu quotidiano e moldando o pensamento de toda a equipa (ibidem, 2017, p. 7). Em vez de tentar apenas coagir comportamentos seguros, o desenvolvimento de uma cultura de cibersegurança possibilita uma mudança de mentalidade, promove a consciência da segurança e a perceção do risco e solidifica a cultura organizacional, esperando-se que os colaboradores entendam as políticas de cibersegurança como diretrizes e não como regras (ibidem, 2017, p. 7).

A constituição de uma cultura de cibersegurança sólida é a solução que permite obter uma mudança duradoura, alcançada através da consciencialização, formação e educação dos colaboradores em matéria de cibersegurança (Gonçalves, 2019, p. 38). Acredita-se que quanto mais preparados estiverem os colaboradores, mais resiliente será a organização, o que significa que a adoção de uma atitude preventiva poderá ajudar a mitigar a ocorrência de ciberataques (ibidem, 2019, p. 38).

Segundo Fisher *et al.* (2021), é necessário criar uma cultura centrada na cibersegurança em todas as organizações, para que todos os colaboradores compreendam e aceitem que a cibersegurança é uma prioridade e que podem ter um papel ativo na defesa cibernética da própria organização (p. 128). Embora os colabores sejam a maior vulnerabilidade, constituem também a maior defesa para mitigar os ciberataques quando lhes são fornecidas as ferramentas e recursos necessários (ibidem, 2021, p. 128).

Neste sentido, podem ser tomadas medidas de prevenção específicas em função dos diferentes tipos de ataque, entre os quais se destacam:

- **Prevenção de *Phishing***

Segundo o *Relatório Riscos & Conflitos*, ao nível do comportamento individual, as medidas de prevenção incluem não clicar em *links*, anexos de *e-mails* ou SMS suspeitos, verificar a origem dos *e-mails*, não partilhar dados sensíveis requisitados por *e-mail* e confirmar os pedidos de transferências bancárias noutras fontes (Centro Nacional de Cibersegurança, 2023, p. 92). Ao nível do comportamento organizacional, deve-se desenvolver ações de sensibilização contra a engenharia social junto dos colaboradores, realizar simulações de *phishing*, aplicar as melhores práticas e *standards* de segurança no que toca à configuração do *e-mail* organizacional e monitorizar estas ações através de políticas de segurança estabelecidas (ibidem, 2023, p. 92).

Por sua vez, o *2023 Cyber Security Report* sublinha que se deve confirmar sempre a linguagem utilizada, dado que, em ataques de *phishing*, os *hackers* geralmente cometem erros gramaticais (Check Point, 2023a). Além disso, nunca se deve partilhar as credenciais e deve-se desconfiar sempre dos *e-mails* de redefinição de *passwords* (ibidem, 2023). Do ponto de vista organizacional, deve-se educar os colaboradores sobre tendências atuais de *phishing*, assim como implantar uma solução anti-*phishing* automatizada capaz de identificar e bloquear conteúdos de *phishing* em todos os serviços e plataformas da organização (ibidem, 2023).

- **Prevenção de *Ransomware***

Tanto para o comportamento individual como para o comportamento organizacional, o *Relatório Riscos & Conflitos* recomenda salvaguardar cópias de segurança em localização secundária e desconectada da rede, manter o antivírus atualizado, evitar aceder a *websites* sem garantias de segurança e não utilizar dispositivos USB de origem desconhecida (Centro Nacional de Cibersegurança, 2023, p. 92). Tal como no *phishing*, recomenda-se que, ao nível das organizações, haja uma formação dos colaboradores e uma monitorização das ações através de políticas de segurança estabelecidas (ibidem, 2023, p. 92).

A Check Point (2023a) acredita que uma solução de salvaguarda de dados robusta e segura é uma forma eficaz de mitigar o impacto de um ataque de *ransomware*. De mencionar a importância de manter os computadores atualizados e aplicar *patches* de segurança, bem como reforçar a autenticação do utilizador, através da aplicação de uma política de *password* forte e da sensibilização dos colaboradores sobre a questão (ibidem, 2023). A implementação de soluções anti-*ransomware* é outra recomendação fundamental, no sentido em que monitorizam programas

em execução num computador com o intuito de identificar comportamentos suspeitos e, se estes comportamentos forem detetados, o programa pode tomar medidas para parar a encriptação antes que mais danos possam ser efetuados (ibidem, 2023). Por último, em contexto organizacional, revela-se fundamental utilizar uma melhor prevenção de ameaças, através de medidas como verificar e monitorizar os *e-mails* e analisar e monitorizar a atividade dos ficheiros (ibidem, 2023).

- **Prevenção de Fraude *online***

O *Relatório Riscos & Conflitos* sublinha que se deve desconfiar de ofertas consideradas demasiado boas para serem verdade, não partilhar dados pessoais em plataformas não reconhecidas, não transferir dinheiro sem confirmar a fiabilidade do destinatário, desconfiar de solicitações de alteração das confirmações de *apps*, como a *MBWay*, utilizar carteiras virtuais ou cartões temporários em pagamentos *online*, confirmar a veracidade dos *websites* e priorizar os que utilizam HTTPS, acrescendo, no caso do comportamento organizacional, a sensibilização dos colaboradores, a garantia de que confirmam o destino e a necessidade das transferências bancárias solicitadas e, ainda, a monitorização das ações através de políticas de segurança estabelecidas (Centro Nacional de Cibersegurança, 2023, p. 92).

Fundamentado num guia de cibersegurança para as PMEs, a ENISA (2021) fornece 12 medidas concretas de alto nível sobre a melhor forma de proteger as empresas, sendo elas:

- Desenvolver uma boa cultura de cibersegurança, procurando atribuir responsabilidade de gestão, obter a aceitação dos colaboradores, realizar auditorias de cibersegurança, publicar políticas de cibersegurança e promover a proteção de dados;
- Proporcionar a formação adequada aos colaboradores, por forma a garantir que saibam reconhecer e lidar com diversas ciberameaças;
- Garantir uma gestão eficaz por parte dos fornecedores;
- Desenvolver um plano de resposta a incidentes assente em orientações, papéis e responsabilidades claras e documentadas;
- Proteger o acesso aos sistemas, através da definição de *passwords* fortes e seguras;
- Proteger os dispositivos, procurando manter o *software* atualizado, utilizar um antivírus, utilizar ferramentas de proteção de correio eletrónico e da *web* e encriptar os dados;
- Garantir a segurança da rede, através da implementação de gestão de dispositivos móveis, da utilização de *firewalls* e da revisão de soluções de acesso remoto;
- Melhorar a segurança física dos dispositivos e documentos importantes;
- Proteger os *backups*, para garantir a recuperação de informação importante para a organização;

- Trabalhar na *cloud*.

Numa abordagem geral, o *2023 Cyber Security Report* revela que as violações de dados podem ser evitadas através de um conjunto de medidas, sendo elas (Check Point, 2023a):

a) Formar e sensibilizar os colaboradores para tomar precauções de segurança;
b) Criar uma *password* segura e alterá-la frequentemente para impedir o acesso;
c) Reduzir o acesso aos dados;
d) Confirmar se os vendedores têm os protocolos de segurança ativados para impedir o acesso dos *hackers* através da sua rede;
e) Utilizar computadores e dispositivos encriptados;
f) Criar uma *cloud* interna à organização.

No mais recente Relatório Semestral de Cibersegurança 2023, a Check Point acrescenta um conjunto de ações que as organizações podem implementar para minimizar a exposição ao risco e os potenciais impactos de um ciberataque, nomeadamente (Check Point, 2023b, pp. 44-45):

a) Implementar uma solução de cópia de segurança de dados robusta e segura;
b) Manter os *patches* atualizados;
c) Implementar soluções anti-*ransomware*, que detetem comportamentos suspeitos;
d) Privilegiar a prevenção em detrimento da deteção, através de mecanismos automatizados de ameaças na organização, incluindo a verificação e monitorização de *e-mails* e da atividade de ficheiros suspeitos.

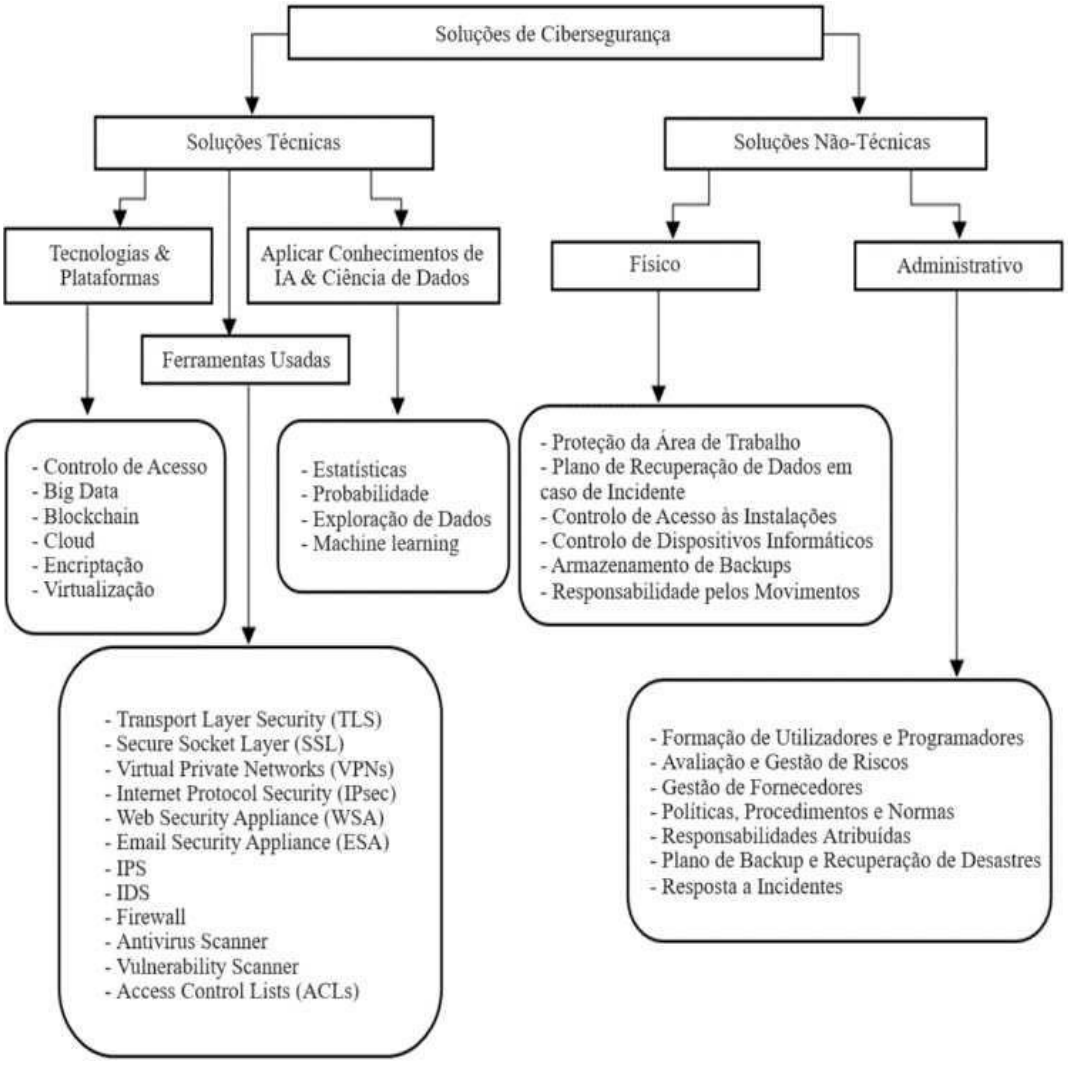
Por sua vez, Aslan *et al.* (2023) propõem um conjunto de soluções de segurança aplicadas no âmbito da cibersegurança, esquematizado na Figura 2. O esquema apresenta as soluções divididas em duas categorias, nomeadamente técnicas e não-técnicas (ibidem, 2023, p. 32).

Por um lado, as soluções não-técnicas estão subdivididas em físicas – incluindo proteção da área de trabalho, plano de recuperação de dados em caso de incidente, controlo de acesso às instalações, controlo de dispositivos informáticos, armazenamento de *backups* e responsabilidade pelos movimentos – e em administrativas – integrando políticas, procedimentos, normas, avaliação de riscos, gestão de fornecedores, responsabilidades atribuídas e formação (Aslan *et al.*, 2023, p. 32).

No que se refere às soluções técnicas, estas subdividem-se em três categorias, sendo a primeira referente a tecnologias e plataformas, incluindo: controlo de acesso, que restringe o acesso aos dados, aumentando a segurança ao mesmo tempo que diminui a possibilidade de ataque

remoto; *big data*, que permite analisar uma grande quantidade de dados com o intuito de descobrir padrões desconhecidos, bem como características maliciosas de ataques; *blockchain*, que ajuda não só a validar a consistência dos dados, como também a detetar alguns ataques complexos; *cloud*, que possibilita uma gestão proativa de ameaças, segurança avançada de dados, escalabilidade, alta disponibilidade e recuperação eficiente de dados; encriptação; e virtualização, que separa as aplicações de *software* dos componentes de *hardware*, aumentando a usabilidade do *software*, diminuindo o custo e reduzindo o tempo de paragem em caso de ciberataque (Aslan *et al.*, 2023, pp. 32-33). A segunda categoria diz respeito a ferramentas utilizadas, integrando instrumentos de segurança como VPNs, IPsec, IDS ou *firewalls* (ibidem, 2023, p. 33). Por último, a categoria inerente à aplicação de Inteligência Artificial e *Data Sciente* engloba estatísticas, probabilidade, exploração de dados e *machine learning* (ibidem, 2023, p. 34).

Figura 2: Soluções técnicas e não-técnicas da Cibersegurança (adaptado de Aslan *et al.*, 2023)



1.10. Desafios, ameaças e tendências atuais

Quando se trata de garantir a segurança cibernética dentro de uma organização, Hussain *et al.* (2020) acreditam que é possível assistir-se a numerosos desafios. Um dos desafios comummente enfrentado pelas organizações é a implementação de uma governação adequada em matéria de cibersegurança, considerando os diversos fatores que necessitam de ser abordados (ibidem, 2020, pp. 4-5). Uma má governação pode gerar um impacto significativo para a organização, resultando num conjunto de vulnerabilidades que podem ser exploradas pelos *hackers* (ibidem, 2020, pp. 4-5). Outro dos desafios apontados diz respeito à gestão adequada dos riscos e à necessidade de ser proativo, revelando-se absolutamente essencial no seio de uma organização, no sentido em que a gestão inadequada do risco pode contribuir para perdas financeiras significativas (ibidem, 2020, pp. 4-5). O último desafio mencionado por Hussain *et al.* (2020) consiste na falta de cultura e consciência das organizações no que toca à cibersegurança, podendo resultar numa aplicação deficiente da segurança cibernética e, consequentemente, numa vulnerabilidade a ser explorada pelos *hackers* (pp. 4-5).

Em termos de desafios para identificar ataques no domínio da cibersegurança, Aslan *et al.* (2019) sublinham, entre outros, a necessidade de um período de tempo alargado para conceber um sistema seguro, a dificuldade em criar, armazenar e distribuir informação confidencial, o desafio em detetar e prevenir ataques desconhecidos, a complexidade de classificar milhões de ligações de rede e proteger múltiplos componentes, a perda de controlo sobre os dados e, ainda, a dificuldade de aplicar conhecimentos de domínio para análise automatizada (pp. 34-35).

O estudo desenvolvido por Hussain *et al.* (2020) foca-se igualmente nas ameaças emergentes que são consideradas um dos fatores mais problemáticos no que toca à cibersegurança (p. 5). A primeira ameaça identificada diz respeito à *Cloud Computing*, uma vez que tem o potencial de enfraquecer a infraestrutura das organizações, dependendo, em larga medida, da capacidade de segurança dos Provedores de Serviços (ibidem, 2020, p. 5). Segue-se a *Internet of Things* (IoT), que apresenta riscos significativos de exploração, embora seja considerado um grande benefício para a evolução da tecnologia (ibidem, 2020, p. 5). Por último, identificou-se como ameaça os *Smartphones*, uma vez que o número de utilizadores com dispositivos sem fios que permitem a interligação entre todas as pessoas, em qualquer momento e em qualquer local do mundo, está a aumentar consideravelmente (ibidem, 2020, p. 5).

Por sua vez, o *Relatório Riscos & Conflitos* apresenta as principais ameaças no contexto da cibersegurança durante o ano de 2022, em resultado do inquérito *Perceção de risco no ciberespaço de interesse nacional 2022/2023* (Centro Nacional de Cibersegurança, 2023, p. 71).

Foi possível apurar as seguintes conclusões: a) a pandemia provocada pela Covid-19 e a guerra na Ucrânia influenciaram a elevada perceção de que aumentou o risco de uma organização sofrer um ciberataque, tendência que se perspetiva igualmente para 2023; b) o *ransomware* e o *phishing*/ *smishing* constituíram-se como as ciberameaças mais relevantes em 2022, perspetivando igualmente para 2023; c) os cibercriminosos e os atores estatais foram apontados como os principais agentes de ameaça em 2022, perspetivando igualmente para 2023; e d) a *Cloud Computing* foi percecionada como a tecnologia emergente mais desafiante no contexto da cibersegurança em 2022, sendo que a Inteligência Artificial tende a ganhar relevância em 2023 (ibidem, 2023, p. 76).

No que se refere a tendências, o *Tech Trends 2023* revela que a própria cibersegurança é uma das principais tendências a nível tecnológico apontadas para 2023 (Rao *et al.*, 2022, p. 60). Adicionalmente, o relatório *Top 7 Trends Shaping Digital Transformation in 2023* demonstra que este ano vai ser caracterizado por um aumento do investimento em cibersegurança por parte das empresas, estando esta cada vez mais integrada para proteger as organizações da complexidade crescente das ameaças que lhe são inerentes (MuleSoft, 2022, pp. 19-21).

Segundo o *2023 Global Future of Cyber Survey*, no presente ano as organizações deverão ter especial atenção a cinco tecnologias de transformação digital aquando da implementação de futuras estratégias de cibersegurança, nomeadamente *Cloud*, Análise de Dados, Tecnologia Operacional, Inteligência Artificial e 5G (Deloitte, 2022, p. 10).

Para o início de 2023, a ENISA revela as principais tendências observadas no panorama europeu de ciberameaças, entre as quais se destacam: a) o *ransomware* e os ataques de negação de serviço ocuparam os primeiros lugares no *ranking* das principais ameaças; b) o aumento da utilização de ferramentas legítimas pelos *hackers*, dificultando a identificação de atividades suspeitas; c) a emergência da geopolítica como área de interesse para as operações cibernéticas; d) o *phishing* mantém-se como o vetor mais comum de acesso inicial; e) o comprometimento do correio eletrónico empresarial continua a ser um dos meios preferidos dos *hackers* para obterem ganhos financeiros; f) o aumento significativo do comprometimento de dados face aos dois anos anteriores; g) a emergência de *chatbots* de inteligência artificial generativa e a sua adoção exponencial, como é o caso do ChatGPT; h) a maior sofisticação e complexidade dos ataques DDoS; i) a manipulação de informação através de Inteligência Artificial continua a ser um motivo de preocupação; e j) o interesse crescente em ataques a cadeias de abastecimento, utilizando os colaboradores como pontos de entrada (Lella *et al.*, 2023, pp. 9-10).

O *Relatório Riscos & Conflitos*, por sua vez, apresenta um conjunto de tendências, a nível internacional, que surgem em 2022 e que poderão perspetivar os anos 2023 e 2024 no âmbito da cibersegurança, nomeadamente: a) *hacktivismo* no âmbito de conflitos ou movimentos de protesto, motivado, sobretudo, pela guerra entre a Rússia e a Ucrânia; b) aumento dos volumes de tráfego direcionados para ataques DDoS; c) continuação de esforços para aceder e explorar vulnerabilidades *zero-day*; e d) ameaças a sistemas de controlo industrial ou tecnologias operacionais (Centro Nacional de Cibersegurança, 2023, pp. 82-84). Ao nível das principais tendências nacionais, o *Relatório Riscos & Conflitos* destaca: a) o incremento do nível de ameaça devido a uma maior "profissionalização" do cibercrime e das repercussões da guerra na Ucrânia; b) a crescente relevância de ameaças como o *ransomware*, o DDoS, o *malware* de furto de credenciais, o *smishing*/ *vishing*/ *spoofing*, ataques baseados em protocolos de pagamentos *contactless*, de maior utilização após a pandemia, e variados tipos de intrusões (ou tentativas), dada a persistência da guerra na Ucrânia; e c) a utilização da Inteligência Artificial como instrumento de acesso facilitado à cibercriminalidade (ibidem, 2023, pp. 86-87). Na sequência das tendências apresentadas no domínio da cibersegurança, o *Relatório Riscos & Conflitos* enumera um conjunto de desafios ao ciberespaço de interesse nacional, entre os quais: a) insuficiente consciência das organizações sobre os seus ativos conectados em rede, devido à emergência de tecnologias como IoT, *cloud computing* ou 5G, dificultado a implementação das medidas necessárias de prevenção dos ciberataques; b) aumento do recurso ao ciberespaço por parte de agentes de ameaça de elevada sofisticação; c) insuficiente literacia digital da sociedade; d) escassez de recursos humanos especializados em cibersegurança nas organizações; e) aumento generalizado das ciberameaças que pode superar os recursos nacionais para a sua prevenção e mitigação; f) falta de uma visibilidade integrada, holística e de carácter permanente sobre infraestruturas críticas e serviços essenciais; e g) insuficiente compreensão da componente não técnica da cibersegurança por parte de algumas organizações (ibidem, 2023, pp. 87-88).

Em termos de tendências para a próxima geração de tecnologia, Hwang *et al.* (2022) acreditam que a implementação dos conceitos *Zero Trust* e SOAR – que passa por um processo de verificação de ID antes de conceder direitos de acesso a todos os objetos que desejam aceder ao sistema –, tornar-se-ão o centro do desenvolvimento da quinta geração da cibersegurança (p. 2). Além disso, de acordo com as tendências de convergência de cibersegurança, a tecnologia de segurança cibernética está a ser desenvolvida principalmente nas áreas de *home city*, rede *wireless*, aplicações, tecnologia de autenticação, rede *wired*, vulnerabilidade de segurança e análise e controlo de ameaças (ibidem, 2022, pp. 9-10).

Importa mencionar as seis tendências apontadas pela Towerwall para 2023, sendo elas: a) maior privacidade dos dados pessoais dos cidadãos, bem como maior pressão regulatória por parte dos governos a nível mundial; b) substituição das *Virtual Private Networks* pelo modelo *Zero Trust*, uma abordagem altamente segura em que os utilizadores são continuadamente validados, reavaliados e reautorizados, utilizando múltiplos métodos de autenticação; c) crescente utilização de ferramentas de deteção e resposta a ameaças cibernéticas baseadas na *cloud* e na Inteligência Artificial; d) aumento da procura de ferramentas, serviços e questionários de fornecedores que possam ajudar a catalogar e monitorizar os riscos cibernéticos de terceiros; e) crescente procura de empresas de consultoria com capacidade de gerir as operações de cibersegurança internas de uma organização; e f) o seguro cibernético irá impulsionar a procura de avaliações de risco, uma vez que as organizações terão a necessidade de provar o nível de maturidade do seu programa de cibersegurança para, assim, negociar uma melhor cobertura do risco (Drolet, 2023).

Por último, revelam-se as tendências apresentadas pelo *2023 Cyber Security Report* relativamente ao ano anterior, nomeadamente: a) a guerra entre a Rússia e a Ucrânia provocou um aumento significativo dos ciberataques em 2022, sendo que o *hacktivismo* e a utilização de *malware* destrutivo por grupos apoiados pelo Estado e entidades independentes tornaram-se mais prevalecentes a nível global; b) aumento significativo da utilização de *wipers* – *malwares* destrutivos, concebidos para infligir danos com potencial limitado de ganhos financeiros para os *hackers*; c) os agentes de ameaças estão a desenvolver e aperfeiçoar as suas técnicas de ataque, as quais dependem cada vez menos da utilização de *malware* personalizado e passam a utilizar ferramentas legítimas; d) mudança de foco da encriptação para a extorsão de dados em casos de *ransomware*; e) aumento do número de ataques através de aplicações móveis bem conhecidas, confiáveis e amplamente utilizadas; e f) a *cloud* tem vindo a tornar-se fonte e alvo de violações de segurança que envolvem uma gestão inadequada do acesso, por vezes combinada com a utilização de credenciais comprometidas (Check Point, 2023a).

2. O estudo da comunicação de crise em contexto de ciberataque e o seu impacto na reputação organizacional

No caso específico da prática de Relações Públicas em contexto de resolução de um ataque informático, diversos autores sublinham a quantidade limitada de investigação académica desenvolvida na área (Kim *et al.*, 2017; Gwebu *et al.*, 2018; Kim & Lee, 2018; Knight & Nurse, 2020; Kuipers & Schonheit, 2021). Não obstante, os ciberataques têm vindo a aumentar em alcance e complexidade, o que significa que a comunicação sobre o incidente é quase tão importante como a gestão do próprio incidente (Sapriel, 2021, p. 2).

Observando a enorme quantidade de casos de violação da cibersegurança, Kim e Lee (2018) acreditam que as pessoas têm vindo a desconfiar cada vez mais da competência das organizações (p. 2). Estando ciente de que um incidente cibernético pode potencialmente transformar-se numa crise – quando aparece nos órgãos de comunicação social e os *stakeholders* começam a reagir –, as empresas devem procurar desenvolver ativamente uma comunicação eficaz com o público para diminuir e minimizar os danos à sua reputação (Wang & Park, 2017, p. 137). Posto isto, a maioria das empresas considera estratégico envolver a função de Relações Públicas na sua abordagem de gestão de riscos cibernéticos, seja antes, durante ou após o incidente ocorrer (Mpholo, 2022).

Embora os profissionais de Relações Públicas não consigam necessariamente resolver todos os aspetos responsáveis por tais crises de violação de segurança de dados, podem e servem, muitas vezes, como pontes de comunicação entre uma organização, os seus *stakeholders* e os órgãos de comunicação social (Kim *et al.*, 2017, p. 2). Para as equipas de resposta a ciberataques, a comunicação e a divulgação desempenham um papel particularmente significativo na partilha de informação, na construção de relações e na promoção da confiança, sendo importante considerar a comunicação como uma iniciativa estratégica da organização (Manley & Mclntire, 2021, p. 3). Contudo, o principal desafio e risco na comunicação sobre ciberataques reside exatamente na forma de divulgar a informação (Ministry of Interior, Republic of Serbia, 2019, p. 2).

Segundo Wang e Park (2017), o tratamento eficaz dos incidentes de cibersegurança é essencial para o resultado final e para a capacidade de sobrevivência das empresas, pelo que a comunicação tem uma correlação direta com a reputação e o desempenho empresarial (p. 137). Significa isto que o principal objetivo da utilização de estratégias de comunicação de crise é proteger e manter a reputação organizacional, sendo o *timing* de resposta o fator mais importante para moldar a perceção pública sobre a responsabilidade da organização no tratamento do incidente e, subsequentemente, sobre a sua reputação (ibidem, 2017, p. 139). Esta é uma ideia igualmente defendida por Kelly (2005), que acredita que a melhor forma de agir rapidamente é ter um plano em vigor e implementá-lo nas primeiras vinte e quatro horas após o ataque informático (p. 26). Por sua vez, o Ministério do Interior da República da Sérvia (2019) defende que o primeiro passo é reconhecer o incidente e, posteriormente, decidir como divulgar a informação necessária sem prejudicar a sua própria reputação (p. 2).

Ao reduzir a sua responsabilidade, uma organização pode minimizar o impacto negativo do incidente sobre a sua reputação (Kim & Lee, 2018, p. 16). A investigação levada a cabo por Kuipers e Schonheit (2021) comprova precisamente que admitir a responsabilidade e oferecer

desculpas e compensações tem um efeito mais positivo na recuperação da reputação após uma violação de dados, do que a negação e a diminuição de estratégias (p. 9). Os resultados da investigação revelam que as estratégias de comunicação devem passar por divulgar informação técnica detalhada e exaustiva sobre o incidente, de forma transparente e adotando um comportamento atento e focalizado no público, considerando que as empresas devem sempre encarar os ataques informáticos como incidentes pelos quais são responsáveis, embora se sintam vitimadas pela pirataria informática (ibidem, 2021, p. 9).

Contudo, um estudo desenvolvido por Bentley *et al.* (2017) demonstrou que os reconhecimentos de responsabilidade foram bastante raros em crises de violação de dados, o que poderá ser explicado pelo facto de estes incidentes serem imputados aos *hackers* e, por isso, haver poucos motivos para uma organização aceitar a culpa (p. 9). Além disso, foi possível compreender que as desculpas por crises de violação de dados eram mais suscetíveis de aconselhar os interessados sobre como se protegerem e de convidá-los a contactar a organização, uma vez que estes incidentes exigem frequentemente que os *stakeholders* sejam ativos na resposta à crise – por exemplo, na mudança de *password* ou no cancelamento de cartões de crédito (ibidem, 2017, p. 10). Por sua vez, Gwebu *et al.* (2018) concluíram que a reputação firme é um trunfo importante na proteção do valor de uma organização em situação de ciberataque, o que significa que as empresas de menor reputação sofrem retornos significativos e negativos após comunicar uma violação de segurança, não se verificando tal situação com as empresas de maior reputação (p. 708).

Convictos de que os *media* parecem manipular a perceção dos incidentes cibernéticos, Kim *et al.* (2017) defendem que uma empresa violada deve não só analisar a sua realidade, como também monitorizar a comunicação da crise empresarial e a sua cobertura noticiosa, dado que a atribuição de responsabilidade a uma empresa pode ser modificada pela perceção da gravidade da crise (p. 13).

É neste sentido que diversos autores propõem modelos de gestão da comunicação de crise, tendo por base aquelas que consideram ser as melhores estratégias em contexto de ataque informático. O modelo proposto por Wang e Park (2017) assenta em importantes estratégias de comunicação situacional de crise, tais como negação, diminuição, reconstrução e reforço, assim como o tempo de resposta aos incidentes, que conjuntamente têm um impacto nas perceções do público sobre a responsabilidade pelo tratamento de incidentes e a reputação da organização (p. 143). Por sua vez, Knight e Nurse (2020) apresentam um quadro conceptual para implementar não só antes da crise cibernética, como também durante o próprio incidente (pp. 9-12). No primeiro caso, estabelecem-se as atividades de planeamento que devem ser envolvidas na preparação de

uma eventual violação de dados, incluindo a definição de objetivos pós-incidente, a identificação de uma base de conhecimentos atualizada e a incorporação de parceiros comerciais nos planos (ibidem, 2020, p. 9). O segundo caso centra-se nas atividades necessárias no caso de uma crise de violação de dados, sendo delineado um modelo de decisão de divulgação que apresenta uma série de passos para ajudar a organização a decidir se, o quê, quando e como divulgar um incidente (ibidem, 2020, p. 9).

Segundo a perspetiva de Manley e Mclntire (2021), cada organização deve desenvolver e implementar o seu próprio plano de comunicação de crise, o qual deverá incluir considerações tanto para a comunicação interna como externa, imagem de marca da organização, envio de mensagens para públicos específicos e objetivos de comunicação (p. 3). Embora o planeamento deva ser, idealmente, conduzido de forma pró-ativa, podem existir momentos em que a organização seja obrigada a comunicar de forma reativa (ibidem, 2021, p. 3). O facto de ter um plano de comunicação estabelecido previamente beneficiará a capacidade da organização para lidar com este tipo de incidentes – as equipas funcionarão de forma mais eficiente –, enquanto tenta manter a sua reputação, transmitir uma mensagem simples e consistente e assegurar que a informação exata e oportuna seja divulgada ao público apropriado (ibidem, 2021, p. 3). Além de promover uma comunicação transparente e honesta, revela-se necessário comunicar com os *stakeholders* frequentemente ao longo do ciclo de vida do incidente e assegurar uma revisão e auditoria do plano regularmente (ibidem, 2021, p. 4). De mencionar, ainda, que a gestão dos órgãos de comunicação social é uma componente chave do planeamento da comunicação, sendo importante fornecer informações atempadas e precisas, assim como determinar o que pode ser dito ou o que é conhecido, por forma a contrariar especulações e rumores (ibidem, 2021, p. 9).

De forma mais estruturada, Santos (2021) propõe um Referencial de Comunicação de Crises em Cibersegurança, focado nos vários ciclos comunicacionais que decorrem numa situação de crise – antes, durante e após o incidente (pp. 27-37). Primeiramente, na fase de Identificação, revela-se necessário não só identificar os riscos e ameaças à reputação da organização, as áreas com maior vulnerabilidade a ataques e os agentes intervenientes aquando da crise, mas também monitorizar e analisar a informação em tempo real (ibidem, 2021, p. 27). Segue-se a fase de Planificação, que exige a definição de um plano de comunicação de crise para o cenário que a organização enfrenta, através da implementação de políticas de prevenção e a sua avaliação de forma regular (ibidem, 2021, p. 29). Posteriormente, a fase de Avaliação requer uma análise dos impactos e danos decorrentes da crise, assim como das informações que saem em tempo real, por forma a garantir uma rápida e eficaz análise da situação de crise (ibidem, 2021, p. 31). Por último, na fase de Resposta, é essencial fazer uma análise reflexiva dos factos, por forma a desenvolver

uma mensagem comunicacional que consiga conter, mitigar e reconquistar a confiança na imagem da organização (ibidem, 2021, p. 33).

Por sua vez, também o Centro Nacional de Cibersegurança (2024) apresenta um *Referencial de Comunicação de Risco e de Crise em Cibersegurança*, composto por um conjunto de indicações e recomendações orientadas para as organizações nacionais no âmbito da comunicação em caso de ciberataque (p. 5). O documento encontra-se organizado em três fases consideradas fundamentais no processo de gestão de comunicação de um ciberataque, em função das quais se estabelecem as recomendações necessárias para uma eficaz gestão do incidente (ibidem, 2024, p. 9).

Na primeira fase, que o Centro Nacional de Cibersegurança (2024) intitula de "Preparar a comunicação de uma crise de cibersegurança", as organizações devem não só definir os incidentes e crises de cibersegurança, fazendo uma clara identificação e correta comunicação dos riscos, como devem também estabelecer um plano de comunicação para os vários cenários de risco e crise, baseado em pressupostos como a rapidez, transparência, flexibilidade e unicidade da mensagem (pp. 13-17). Para que o plano seja exequível e útil no momento da sua aplicação, é necessário definir uma equipa de comunicação de crise de cibersegurança, identificar grupos de interesse, desenvolver uma lista de contactos envolvidos na gestão do incidente e que estejam devidamente informados acerca da crise, definir *templates* de comunicação ajustados aos diferentes grupos de interesse, determinar os meios através dos quais a comunicação será feita, definir a estratégia de comunicação durante a mitigação do incidente e, por último, testar o plano de comunicação através de exercícios de simulação (ibidem, 2024, pp. 19-32).

Na segunda fase, intitulada de "Responder eficazmente", o Centro Nacional de Cibersegurança (2024) sugere começar por ativar a equipa de resposta incidentes, incluindo a equipa responsável pela comunicação de crise, devendo-se, posteriormente, reportar o incidente conforme exigido nos regulamentos e contratos, sobretudo às entidades competentes como o CNCS, documentar o incidente com informação detalhada, comunicar o encerramento formal da crise, tanto a nível interno como externo, e recuperar a reputação da organização (pp. 33-43). Para uma eficaz gestão da reputação, deve-se ter em consideração a recuperação desde o início da crise, fomentar a confiança dos *stakeholders* através de ações, envolver os colaboradores, redefinir a agenda através de uma comunicação ativa, cumprir as promessas feitas e ter em atenção os prazos estabelecidos e, ainda, utilizar as "janelas de oportunidade" decorrentes da crise para realizar alterações a longo prazo (ibidem, 2024, pp. 44-46).

A última fase do referencial do Centro Nacional de Cibersegurança (2024), intitulada de "Aprender lições e melhorar", recomenda às organizações fazer uma revisão da crise e avaliação global do plano de comunicação, através da recolha de *feedback* acerca da gestão do incidente, no sentido de apurar o resultado da estratégia e das ações definidas e, assim, melhorar a resiliência e capacidade de resposta da organização em incidentes futuros, procurando atualizar o plano de comunicação com as lições aprendidas (pp. 48-50). Além disso, esta é a fase em que a organização deve monitorizar e rever os riscos a que se encontra exposta, embora esta deva ser uma ação regular e permanente (ibidem, 2024, p. 51).

Por forma a contribuir para a gestão de crise provocada por um ciberataque, Mpholo (2022) sublinha que o profissional de Relações Públicas deve entender de que forma um ataque informático pode prejudicar a reputação da organização – garantindo que os *stakeholders* estão igualmente elucidados –, impulsionar a educação sobre o impacto dos ataques, tanto interna como externamente, e desenvolver uma lista de verificação integrada de incidência de ameaças à segurança cibernética, que forneça atualizações em tempo real sobre possíveis ataques. Além disso, o profissional de Relações Públicas pode também tomar algumas decisões pós-ataque, como sendo: a gestão de reputação através das redes sociais; a criação de uma incidência de FAQs (Perguntas Frequentes), para esclarecimento de eventuais dúvidas sobre o ataque; a publicação de diretrizes de relatórios de incidência em toda a organização, para garantir que todas as informações sobre o ataque sejam divulgadas corretamente; e a realização de análise, avaliação e revisão da reputação pós-incidente (ibidem, 2022).

No que respeita à utilização das redes sociais enquanto instrumento de gestão de crise, Martins (2022) concluiu que, aliado a um conjunto de estratégias definidas pela organização, as redes sociais podem ser benéficas para gerir uma situação de crise como um ciberataque (p. 49). Entre as vantagens inerentes à sua utilização, as redes sociais permitem informar o público de forma mais rápida, além de possibilitar à organização avaliar as reações perante a situação, através dos comentários partilhados pelo público nas publicações efetuadas pela organização (ibidem, 2022, p. 49).

Sob uma perspetiva diferente, a UNITAS desenvolveu um exercício conduzido em torno de um cenário hipotético baseado num ataque informático a um conjunto de infraestruturas financeiras (European Central Bank, 2018, p. 2). Os participantes reconheceram que a partilha de várias formas de informação – informação sobre ameaças e dados sobre incidentes –, a nível europeu, poderia ser melhorada para permitir a rápida recuperação de um incidente que afete a integridade dos dados (ibidem, 2018, p. 2). De mencionar que os participantes salientaram a

importância da formação e sensibilização das equipas de Relações Públicas, para melhorar as suas capacidades de resposta e recuperação de um incidente cibernético grave (ibidem, 2018, p. 2).

Em termos de gestão da relação com os *stakeholders*, Sapriel (2021) defende que para antecipar, prevenir e mitigar as crises, os líderes empresariais e de crise devem ter um sólido domínio do clima em que estão a trabalhar, bem como do cenário dos *stakeholders* em torno de qualquer questão emergente (p. 3). Em caso de ciberataque, onde a investigação e a resolução levam tempo, o envolvimento rápido, ativo e regular dos *stakeholders* revela-se crítico para manter a confiança, sobreviver à crise e possivelmente emergir mais forte (ibidem, 2021, p. 4). Se os intervenientes internos e externos são os pilares da existência das organizações, a rapidez, a transparência e a honestidade são os pilares da credibilidade (ibidem, 2021, p. 8). Posto isto, o mapeamento dos *stakeholders* é o ponto de partida para comunicar de forma sensível e eficaz e, assim, evitar prejudicar a reputação organizacional (ibidem, 2021, p. 8).

Capítulo III – Investigação Empírica

1. Desenho de pesquisa

A presente dissertação tem como principal foco a perspetiva de diferentes profissionais e especialistas das áreas da cibersegurança e da comunicação sobre o tema da prevenção e resposta a um ciberataque. O principal objetivo passa pela criação de conhecimento especializado e em profundidade sobre o tema no contexto português que, por sua vez, permitirá não só construir um quadro teórico na área, como elaborar um manual de boas práticas.

Por forma a orientar a pesquisa e fornecer uma compreensão clara do fenómeno em estudo, estabeleceu-se a seguinte questão de partida: ***"Como é que os profissionais de Relações Públicas podem contribuir para a preparação das organizações em situação de ciberataque, no contexto português?"***

Com o intuito de conduzir a investigação e, assim, dar resposta à questão delineada previamente, foram formulados os seguintes objetivos específicos de investigação:

1. Desenvolver um quadro teórico sobre Cibersegurança no contexto das Relações Públicas em Portugal;
2. Compreender a perspetiva de profissionais de Relações Públicas sobre o papel que desempenham numa situação de ciberataque;

3. Elaborar uma proposta de guia de boas práticas de prevenção e resposta a um ciberataque a implementar pelos profissionais de Relações Públicas nas organizações.

2. Abordagem metodológica

Em função dos objetivos do presente estudo, optou-se por uma abordagem metodológica qualitativa, com recurso a técnicas de cariz qualitativo, nomeadamente a entrevista e consequente análise de conteúdo qualitativa.

Associada a uma visão interpretativa e construtiva do mundo, a abordagem qualitativa tem em vista explorar as intenções, motivações e experiências subjetivas dos indivíduos, numa ótica de interpretação da realidade social do ponto de vista dos indivíduos que a integram (Daymon & Holloway, 2005, p. 4). Desafiando a noção de que a realidade social é um dado adquirido, os investigadores interpretativos baseiam-se no construtivismo social – a ideia de que a realidade em que vivemos é construída ao longo do tempo através da comunicação, das nossas interações com os outros e da nossa história partilhada (ibidem, 2005, pp. 4-5).

No âmbito das ciências sociais, esta abordagem metodológica está direcionada para procedimentos centrados na investigação em profundidade (Espírito Santo, 2015, p. 27). Contrariamente à abordagem quantitativa, que se preocupa com a análise numérica, a presente abordagem prende-se mais com o estudo das palavras, baseando-se na interpretação, inferência e indução (Bryman, 2012, p. 380). Também Creswell (2003) entende o método qualitativo como fortemente intuitivo, no qual o investigador gera significado através dos dados recolhidos no campo (p. 9). De forma resumida, a abordagem qualitativa pauta-se pela abertura, flexibilidade e subjetividade dos seus procedimentos (Blaikie, 2010, p. 215).

Assim sendo, na presente investigação, a escolha da abordagem metodológica qualitativa recaiu sobre a necessidade de explorar e analisar os pontos de vista de diferentes especialistas e profissionais quer de Cibersegurança, quer de Relações Públicas, considerando as suas experiências pessoais no que respeita ao tema em estudo.

3. Instrumento de recolha de dados

3.1. Entrevistas

Por forma a dar resposta à questão de partida, optou-se por realizar, numa primeira instância da recolha de dados, um conjunto de entrevistas a profissionais e especialistas na área das Relações Públicas e na área da Cibersegurança. No primeiro caso, procedeu-se à realização de

entrevistas com especialistas em comunicação de crise, assim como representantes de comunicação de organizações que tenham enfrentado recentemente uma situação de ciberataque. No segundo caso, o critério de seleção dos entrevistados baseou-se na sua especialização e experiência profissional no ramo da cibersegurança.

No âmbito das abordagens qualitativas à investigação em Relações Públicas, as entrevistas constituem-se como um instrumento útil de recolha de dados por permitirem explorar as perspetivas e perceções de vários indivíduos (Daymon & Holloway, 2005, p. 166). O seu valor reside no interesse em compreender a experiência vivenciada por outros indivíduos e, consequentemente, o significado que conferem a essa experiência (Seidman, 2006, p. 9).

Segundo Bryman (2012), a entrevista é provavelmente o método mais amplamente utilizado na investigação qualitativa, dado o seu nível de flexibilidade (p. 469). Perante esta flexibilidade, o investigador tem uma maior liberdade para introduzir novas questões ou solicitar mais informações consoante o decorrer da conversa, sem estar limitado a uma padronização de alternativas (Daymon & Holloway, 2005, p. 167). Do mesmo modo, os entrevistados podem explorar as suas ideias com maior profundidade ou exercer um maior controlo sobre a entrevista, garantindo uma maior espontaneidade das suas respostas (ibidem, 2005, p. 167).

No que se refere à natureza da sua estrutura, as entrevistas podem ser não estruturadas, semiestruturadas ou estruturadas, sendo que os investigadores qualitativos excluem, geralmente, a última opção por enfraquecer a flexibilidade que é tão valorizada numa investigação qualitativa (Daymon & Holloway, 2005, p. 169). Na presente dissertação, optou-se pela entrevista semiestruturada, que Bryman (2012) entende como um conjunto de questões definidas previamente, havendo a possibilidade de o investigador fazer perguntas que não estão incluídas no guião sempre que o considerar pertinente (p. 471).

Numa entrevista semiestruturada, o guião é formulado em função das áreas temáticas a abordar e das linhas de investigação a seguir, embora exista flexibilidade na sequência das perguntas colocadas, uma vez que depende do processo de cada entrevista e das respostas de cada entrevistado (Daymon & Holloway, 2005, p. 171). O objetivo passa por recolher dados semelhantes de diferentes entrevistados, pelo que é necessário o guião centrar-se em aspetos específicos do tema a analisar (ibidem, 2005, p. 171).

Para a realização das entrevistas semiestruturadas, procedeu-se à elaboração de dois guiões de entrevista com questões ligeiramente diferentes, visto que o fenómeno em estudo integra duas áreas distintas: Cibersegurança e Relações Públicas. Assim sendo, esta distinção decorre da área

profissional dos entrevistados, bem como dos objetivos que se pretende explorar através da realização de cada entrevista.

Ambos os guiões foram elaborados tendo por base um conjunto de tópicos orientadores. No caso do guião direcionado aos profissionais de Cibersegurança, estabeleceram-se os seguintes tópicos:

- **Evolução dos ciberataques em Portugal**: procurou-se compreender de que forma têm evoluído os ciberataques no país, quer em termos do seu impacto, quer em termos da sua magnitude.
- **Fatores que motivaram o aumento do número de ciberataques desde 2020**: procurou-se compreender os fatores que motivaram o aumento significativo dos ciberataques desde, sensivelmente, 2020, em Portugal.
- **Atual panorama de ciberataques em Portugal**: procurou-se compreender os tipos de ataques mais frequentes, os setores de atividade mais atacados e os riscos inerentes às organizações mais verificados.
- **Importância de uma organização segura**: procurou-se compreender o que assegura e o que previne à organização uma maior aposta na cibersegurança.
- **Maturidade das empresas portuguesas em cibersegurança**: procurou-se compreender o atual nível de maturidade das empresas portuguesas no que respeita à aposta em políticas de cibersegurança.
- **Medidas de segurança**: procurou-se compreender as medidas e ações de segurança que as organizações devem implementar em situação de ciberataque, sobretudo numa ótica de prevenção.
- **Tendências e desafios em cibersegurança**: procurou-se compreender não só as principais tendências e desafios atuais que têm impactado a área da cibersegurança, como também aqueles que, futuramente, poderão ser uma preocupação para as organizações.
- **Futuro dos ciberataques em Portugal**: procurou-se compreender qual a evolução futura dos ciberataques, sobretudo em Portugal.

No que respeita ao guião desenvolvido para os profissionais de Relações Públicas, estabeleceram-se os seguintes tópicos:

- **Situação de crise enfrentada pela empresa alvo de um ciberataque**[1]: procurou-se compreender qual o modo de atuação da organização perante o incidente, bem como as implicações que o ciberataque provocou à organização.
- **Importância da comunicação de crise numa situação de ciberataque**: procurou-se compreender o que assegura e o que previne uma adequada gestão de crise e consequente comunicação, tanto a nível interno, como a nível externo à organização.
- **Papel do profissional de Relações Públicas numa situação de ciberataque**: procurou-se compreender a importância de um profissional de Relações Públicas na gestão de uma situação de ciberataque, quer a nível interno, quer a nível externo à organização.
- **Desafios enfrentados pelo profissional de Relações Públicas numa situação de ciberataque**: procurou-se compreender os principais desafios que o profissional de Relações Públicas enfrenta aquando da execução da sua função numa situação de ciberataque, considerando as características particulares de uma crise provocada por um ataque cibernético.
- **Medidas de comunicação em situação de ciberataque**: procurou-se compreender as medidas e ações de comunicação que as organizações devem implementar em situação de ciberataque, seja antes, durante ou após a crise.
- **Importância dos *stakeholders* em situação de ciberataque**: procurou-se compreender a importância de todos os *stakeholders* da organização no processo de gestão de um incidente cibernético.
- **Implicações do ciberataque na reputação organizacional**: procurou-se compreender se a ocorrência de um ciberataque poderá ter implicações na reputação da organização e que tipo de implicações são essas.
- **Implicações do fenómeno de ciberataque na área das Relações Públicas**: procurou-se compreender se, de alguma forma, o fenómeno de ciberataque vai impactar aquilo que era, até então, a atividade de Relações Públicas.

Posto isto, no âmbito da Cibersegurança, foram entrevistados seis profissionais, constituindo uma amostra variada em termos das suas funções, tal como nos revela o painel de entrevistados apresentado na Tabela 12. Por um lado, Rui Duro, Mauro Almeida e Duarte Freitas representam três grandes entidades prestadoras de serviços de cibersegurança em Portugal – *Check*

[1] Questão colocada somente aos representantes de comunicação de organizações que tenham enfrentado recentemente uma situação de ciberataque.

Point Software Technologies, NTT Data Portugal e IBM Portugal, respetivamente. Numa vertente governamental, procedeu-se à realização de uma entrevista com António Gameiro Marques, Diretor-Geral do Gabinete Nacional de Segurança, e Pedro Verdelho, Diretor do Gabinete Nacional de Coordenação na área do Cibercrime, da Procuradoria-Geral da República. Por sua vez, revelou-se pertinente a realização de uma entrevista com um membro do Centro Nacional de Cibersegurança e, tratando-se de um tema que conjuga a segurança cibernética com a comunicação, a escolha incidiu sobre Pedro Mendonça, consultor no CNCS e responsável pelo Observatório de Cibersegurança.

Tabela 12: Painel de entrevistados na área da Cibersegurança

Nome do entrevistado	**Função**	**Data**	**Hora**	**Duração**	**Recolha da entrevista**
Rui Duro	Country Manager da Check Point Software Technologies em Portugal	27 de junho de 2023	10h00	1 hora	*Online*, via Microsoft Teams
Mauro Almeida	Head of Cyber Security da NTT Data Portugal	27 de junho de 2023	12h00	45 minutos	*Online*, via Zoom
Pedro Mendonça	Consultor no Centro Nacional de Cibersegurança, responsável pelo Observatório de Cibersegurança	7 de julho de 2023	11h00	45 minutos	*Online*, via Microsoft Teams
António Gameiro Marques	Diretor-Geral do Gabinete Nacional de Segurança	10 de julho de 2023	19h00	1 hora	*Online*, via Microsoft Teams
Pedro Verdelho	Diretor do Gabinete Nacional de Coordenação na área do Cibercrime, da Procuradoria-Geral da República	18 de julho de 2023	11h00	45 minutos	*Online*, via Microsoft Teams
Duarte Freitas	Responsável pelos serviços de cibersegurança na IBM Portugal	25 de julho de 2023	19h15	1 hora	*Online*, via Microsoft Teams

No contexto da área das Relações Públicas, a amostra constituiu igualmente um total de seis profissionais e especialistas da área, como se pode verificar no painel de entrevistados disponível na Tabela 13. Numa primeira instância, procurou-se entrevistar duas especialistas em comunicação de crise, nomeadamente Alexandra Abreu Loureiro, representante do Brunswick Group em Portugal e nos países lusófonos, assim como Paula Ramos, Diretora de Comunicação Corporativa e Financeira na LLYC. Posteriormente, revelou-se necessário compreender igualmente a perspetiva de representantes de organizações portuguesas que tivessem sido alvo de

um ciberataque recentemente, sendo eles: Carina Sousa Correia, Responsável pela Comunicação Externa da Vodafone Portugal; António Borges, Técnico Superior de Comunicação e Marketing no INEM; Rui Cabrita, Diretor de Comunicação do Grupo EDP; e Anabela Lopes Simões, Responsável pela Comunicação do Grupo Luís Simões.

Tabela 13: Painel de entrevistados na área das Relações Públicas

Nome do entrevistado	**Função**	**Data**	**Hora**	**Duração**	**Recolha da entrevista**
Alexandra Abreu Loureiro	Representante do Brunswick Group em Portugal e nos países lusófonos	26 de junho de 2023	08h30	30 minutos	*Online*, via Zoom
Carina Sousa Correia	Responsável pela Comunicação Externa da Vodafone Portugal	17 de julho de 2023	-	-	*Online*, via *e-mail*
Paula Ramos	Diretora de Comunicação Corporativa e Financeira na LLYC	31 de julho de 2023	13h00	45 minutos	*Online*, via Google Meet
António Borges	Técnico Superior de Comunicação e Marketing no INEM	25 de agosto de 2023	10h30	30 minutos	*Online*, via Microsoft Teams
Rui Cabrita	Diretor de Comunicação do Grupo EDP	12 de setembro de 2023	10h00	1 hora	*Online*, via Microsoft Teams
Anabela Lopes Simões	Responsável pela Comunicação do Grupo Luís Simões	2 de novembro de 2023	15h00	1 hora	*Online*, via Microsoft Teams

Na sua totalidade, as entrevistas decorreram entre os meses de junho e novembro de 2023, sendo que os pedidos de entrevista foram efetuados via *e-mail* e via *LinkedIn*. A mensagem dos contactos estabelecidos tinha em vista esclarecer o contexto geral do tema a investigar, bem como o propósito da entrevista.

Todas as entrevistas decorreram em formato *online*, seja via *Zoom*, *Microsoft Teams* ou *Google Meet*, à exceção da entrevista realizada a Carina Sousa Correia que, por motivos de indisponibilidade de horário, optou pelo envio das respostas via *e-mail*.

Por forma a validar a sua participação na entrevista, foi enviado a cada entrevistado um *Protocolo de Investigação*, sendo que todos eles concordaram com a gravação da entrevista, como se pode constatar no Apêndice 1. A gravação das entrevistas permitiu uma transcrição mais

fidedigna das declarações prestadas pelos entrevistados, estando disponível para consulta nos Apêndices 2 a 13.

Importa ressalvar que, na totalidade, foram realizados 33 contactos, dos quais foi possível efetuar 12 entrevistas. No que se refere aos profissionais de Cibersegurança, além dos seis entrevistados, procurou-se contactar, adicionalmente, três empresas prestadoras de serviços de cibersegurança – Claranet Portugal, Noesis Portugal e WhiteHat – e, ainda, um especialista em cibersegurança, embora não se tenha obtido resposta.

No caso dos profissionais de Relações Públicas, destacam-se a Sonae MC, o Grupo Super Bock, o Grupo Impresa e o Ministério da Economia que, embora tenham manifestado interesse em colaborar, até à data não confirmaram disponibilidade para a realização da entrevista. Foram contactados igualmente a TAP Air Portugal, o Estado-Maior-General das Forças Armadas, o Grupo Germano de Sousa, a Altice Portugal e a Agência Lusa, assim como Elsa Lemos, especialista em comunicação de crise, que, por diferentes motivos, demonstraram indisponibilidade para a realização das entrevistas. No que toca às restantes entidades contactadas, nomeadamente Direção-Geral da Saúde, Segurança Social, Global Media Group, Hospital Garcia de Orta, Millennium BCP, Sporting Clube de Portugal e Grupo Visabeira, não foi possível obter resposta.

4. Procedimento de Análise de Conteúdo Qualitativa

Por forma a analisar corretamente os dados recolhidos e, assim, cumprir com os objetivos estabelecidos, procedeu-se à análise de conteúdo qualitativa, um método frequentemente utilizado na análise de documentos e entrevistas.

A análise de conteúdo qualitativa permite descrever, de forma sistemática, o significado do material qualitativo, através da atribuição sucessiva de partes do material a categorias de uma grelha de codificação (Schreier, 2012, p. 1). Esta grelha representa o eixo central da análise, no sentido em que abrange todos os significados que surgem na descrição e interpretação do material (ibidem, 2012, p. 1). O significado não se constituiu como um dado adquirido; pelo contrário, é construído de acordo com a perceção e contexto do investigador (ibidem, 2012, p. 2).

Embora seja de natureza qualitativa, este método engloba também alguns dados quantitativos, seja ao quantificar a consistência da codificação, seja na apresentação dos resultados em formato de frequência (Schreier, 2012, p. 36). Por esse motivo, será feita uma contabilização do número de unidades de registo presentes em cada categoria, por forma a averiguar quais os assuntos mais abordados pelos entrevistados.

As categorias principais – também denominadas dimensões – correspondem aos aspetos em que o investigador pretende centrar a sua análise, sendo definido, para cada uma delas, um conjunto de subcategorias que ajudam a descrevê-las de forma mais específica (Schreier, 2012, pp. 59-60).

Por conseguinte, a grelha de codificação terá de ser estruturada de forma adequada, identificando as dimensões que serão utilizadas para descrever os dados e as respetivas subcategorias a elas subjacentes, existindo três formas de o fazer (Schreier, 2012, pp. 84-94):

- ***Concept-driven way***: categorias baseadas na utilização de conhecimento já existente, antes de consultar os próprios dados. Este conhecimento pode advir de diferentes fontes, como sendo uma teoria, investigação anterior, experiência quotidiana ou lógica;
- ***Data-driven way***: categorias baseadas num processo indutivo, tendo por base os resultados da recolha de dados. Esta estratégia é especialmente útil se o objetivo for analisar o material em profundidade;
- **Combinação das duas estratégias**: esta foi a estratégia adotada no presente estudo, no sentido em que, através do conhecimento pré-existente, estabeleceu-se as categorias que se considerou serem fundamentais, acrescentando-se, na fase de leitura das entrevistas, novas categorias que emergiram da análise dos dados.

A análise dos dados procedeu-se com o auxílio do programa NVIVO, um dos principais *softwares* sugeridos por Schreier (2012) para a análise qualitativa de dados. Este programa foi concebido para apoiar a codificação descritiva e interpretativa dos dados, possível através da criação de uma grelha de codificação que reúne todas as categorias e respetivas subcategorias (Schreier, 2012, p. 245).

Assim sendo, o primeiro passo consistiu na importação de todas as entrevistas para o *software* de análise de dados, por forma a poderem ser analisadas e interpretadas convenientemente – passando a designar-se como unidades de análise (Schreier, 2012, p. 130). Seguiu-se a construção da grelha de codificação, a sua respetiva inserção no *software* e a consequente atribuição das categorias a variadas citações dos entrevistados, designadas por Schreier (2012) como unidades de código. Estas unidades de código correspondem a recortes das unidades de análise que podem ser interpretadas e enquadradas numa subcategoria (Schreier, 2012, p. 131).

Todas as categorias e subcategorias que resultaram desta análise encontram-se explicitadas nos Apêndices 14 e 15. Dado que existem dois grupos distintos de entrevistados, revelou-se necessário elaborar duas grelhas de codificação adequadas a cada um deles, pelo que a sua descrição é apresentada igualmente de forma separada.

Capítulo IV – Apresentação dos resultados

Neste capítulo, apresentam-se, numa primeira instância, os resultados da análise e interpretação das entrevistas realizadas aos profissionais de Cibersegurança, por forma a enquadrar a cibersegurança no contexto da realidade portuguesa, quer a nível da sociedade, quer a nível organizacional. Posteriormente, segue-se a apresentação dos resultados da análise e interpretação das entrevistas realizadas aos profissionais de Relações Públicas, procurando estabelecer uma visão prática da comunicação de crise em situação de ciberataque. O capítulo finaliza com a apresentação de uma proposta de um Guia de Boas Práticas de Prevenção e Resposta a um Ciberataque.

1. O estudo da Cibersegurança no contexto português

Tendo por base o conjunto de dimensões em estudo, é possível constatar que as medidas de segurança e o atual panorama de ciberataques foram as que apresentaram um maior número de unidades de recorte, destacando-se, em larga medida, das restantes, embora este facto seja justificado pelo maior número de subcategorias que constituem estas dimensões.

Tabela 14: Categorias de análise do conjunto de entrevistas realizadas aos profissionais de Cibersegurança

Categorias	**Unidades de recorte**
Evolução dos ciberataques em Portugal	25
Fatores que motivaram o aumento dos ciberataques desde 2020	45
Atual panorama de ciberataques em Portugal	**81**
Importância de uma organização segura	17
Maturidade das empresas portuguesas em cibersegurança	23
Medidas de segurança	**84**
Principais tendências na área da cibersegurança	35
Principais desafios na área da cibersegurança	52
Futuro dos ciberataques em Portugal	32

1.1. Evolução dos ciberataques em Portugal

A evolução dos ciberataques em Portugal enquadrou-se em quatro fases de desenvolvimento, propostas por Alexandrou (2021) na revisão da literatura: a primeira associada a um esforço de natureza experimental que compreende o período entre 1970 e 1980; a segunda que antecede o cibercrime, durante um período compreendido entre 1990 e 2000; a terceira caracterizada pelo desenvolvimento do cibercrime, com origem no início dos anos 2000 e estendendo-se até 2010; e a última fase marcada pela emergência de uma ameaça global, transformada num cenário de guerra cibernética, com início em 2011 até à atualidade.

Tabela 15: Fases de desenvolvimento dos ciberataques

Fases de desenvolvimento dos ciberataques	**Unidades de recorte**
Fase Experimental	2
Pré-Cibercrime	4
Fase de Desenvolvimento do Cibercrime	3
Guerra Cibernética	**16**

De entre o conjunto de fases de desenvolvimento dos ciberataques, existe um destaque atribuído à Guerra Cibernética. Com um valor correspondente a 16 unidades de recorte, esta fase recebeu uma maior atenção por parte dos entrevistados, possivelmente pela maior proximidade temporal dos acontecimentos à nossa realidade presente.

a) Fase Experimental

A primeira fase de desenvolvimento dos ciberataques foi a menos referida pelos entrevistados, o que poderá ser explicado pela distância temporal a que nos encontramos da referida época. Ainda assim, os entrevistados associam esta fase à emergência da *Internet* e dos primeiros dispositivos digitais, pelo que a cibersegurança não assumia ainda uma grande relevância, não existindo, portanto, grandes ciberataques a empresas portuguesas. Não obstante, Duro (2023) sublinha que, devido à baixa proteção e falta de consciência em cibersegurança por parte das empresas portuguesas, Portugal era dos países que mais participava em ataques internacionais.

"[...] a questão da cibersegurança coloca-se a partir do momento em que há Internet – embora ela não se reduza à dimensão da Internet –, dispositivos digitais… Nos primórdios, a preocupação da cibersegurança não era muito evidente e ela vai surgindo depois com o tempo. Os anos 80 eu diria que é uma época, a nível internacional, em que a cibersegurança começa a ganhar cada vez mais relevância" (Mendonça, 2023) (Apêndice 4)

"[...] as empresas portuguesas tinham os seus sistemas [...] reféns e participávamos naqueles ataques de spam, nos ataques de denial-of-service, nos ataques de phishing… Porque, apesar de não haver grandes ataques a companhias portuguesas, [...] havia muitas máquinas em Portugal infetadas, que eram utilizadas para fazer ataques noutras partes do mundo" (Duro, 2023) (Apêndice 2)

b) Pré-Cibercrime

Segue-se a fase correspondente ao Pré-Cibercrime, registando 4 unidades de recorte. Devido à criação das primeiras ligações à *Internet*, os entrevistados caracterizam esta fase pela emergência de alguns ataques, embora rudimentares, e pela implementação de medidas de segurança nas organizações, em parte pela evolução da dimensão do fator humano. Esta é uma fase em que a cibersegurança começa a ganhar uma maior relevância no seio das organizações.

"Eu comecei a trabalhar em cibersegurança nos anos 90. Na altura, o conceito de cibersegurança ainda não existia, mas comecei com a primeira necessidade de algumas organizações se protegerem através de firewalls, uma vez que se começaram a ligar à Internet. [...] Então, já havia uma sensação de que era preciso criar regras, haver políticas de segurança mínimas para que as organizações ficassem protegidas" (Freitas, 2023) (Apêndice 7)

"Primeiro, as grandes ameaças eram programas maliciosos que, ainda hoje, são uma grande ameaça, mas depois começa também a evoluir para a dimensão do fator humano, cada vez mais presente, nomeadamente, com os ataques de phishing – que é algo que começa a evoluir a partir dos anos 90" (Mendonça, 2023) (Apêndice 4)

"[...] tivemos, no longínquo ano de 90 e poucos, alguns ataques, embora muito rudimentares comparados com aquilo que se faz agora. Mas já tínhamos alguns problemas e, na altura, fez-se lá no Instituto [Superior Técnico] talvez das primeiras conferências sobre cibersegurança que houve no país" (Duro, 2023) (Apêndice 2)

c) Fase de Desenvolvimento do Cibercrime

A fase de desenvolvimento do cibercrime foi, igualmente, uma categoria que registou um número reduzido de unidades de registo. Porém, Verdelho (2023) debruçou parte da sua atenção sobre esta fase, esclarecendo que, devido à adoção da *Internet* nas organizações e enquanto ferramenta diária de trabalho, começaram a emergir os ataques informáticos a sistemas de informação.

> *"E só a partir desta altura [fim da primeira década deste século] é que se coloca esta questão dos ataques a sistemas. Já se podia atacar um sistema, mas isso não tinha repercussão, porque as pessoas daquela empresa ficavam com o computador não utilizável durante um dia ou dois, mas não acontecia mais nada. Agora, atacar um sistema informático, por exemplo, de um canal de televisão, ou de um jornal, ou de um banco, isso já tem repercussões em terceiros"* (Verdelho, 2023) (Apêndice 6)

Além disso, a maior consciência sobre cibersegurança permitiu estabelecer uma maior perceção dos serviços que as organizações necessitavam para as ajudar a proteger-se de eventuais ciberataques.

> *"Isso já foi nos anos 2000 e já havia uma definição muito concreta do que seriam os serviços e que maioria de serviços as organizações iriam necessitar"* (Freitas, 2023) (Apêndice 7)

d) Guerra Cibernética

A fase mais atual de desenvolvimento dos ciberataques foi abordada pela totalidade dos entrevistados, sendo a maioria das referências atribuídas ao entrevistado Pedro Verdelho. Segundo os entrevistados, esta fase é caracterizada pelo aumento significativo do número de ciberataques, como consequência natural do contexto atual em que vivemos, e pela complexidade e sofisticação das técnicas utilizadas, assemelhando-se largamente à tendência internacional.

> *"[...] é sabido que os números de ciberataques estão a subir de uma forma permanente, consistente e constante"* (Verdelho, 2023) (Apêndice 6)

> *"Eu acho que entre 2020 e 2022, assistimos a um crescimento progressivo, isto é, técnicas muito mais evoluídas [...] E em termos de quantidade de persistência, claramente também aumentou"* (Freitas, 2023) (Apêndice 7)

"Portugal tem também acompanhado a tendência internacional, ou seja, um aumento do número de ciberataques [...]" (Almeida, 2023) (Apêndice 3)

"Nós estamos integrados num mundo global e, hoje, os ataques em Portugal são iguais e com a mesma dimensão daqueles que ocorrem nos Estados Unidos, em França ou em Espanha, ou em qualquer lado do mundo" (Duro, 2023) (Apêndice 2)

Como o próprio nome indica, estamos perante uma fase que se caracteriza pela emergência da guerra no ciberespaço, através de ações patrocinadas pelos próprios Estados e pela ciberespionagem. Relembrando a perspetiva de Alexandrou (2021), o cibercrime começa a crescer para além do *hacking* e roubo de identidade, transformando-se numa ameaça global mais sofisticada e assemelhando-se a uma silenciosa guerra mundial, que não conhece fronteiras e que diz respeito a todas as nações do planeta (ibidem, 2021, p. 71).

"Isto tem uma parte completamente verdade e outra parte que não é completamente verdade, que recentemente ganhou dimensão, que é a guerra cibernética. A invasão da Ucrânia pela Rússia tem uma subcamada que nem sempre faz notícia que é a guerra digital também. Antes de a guerra começar no terreno, já a guerra digital tinha começado. [...] Esta é uma realidade importante também, mas tem mais que ver com ciberdefesa e ciberguerra" (Verdelho, 2023) (Apêndice 6)

"O ciberespaço é um espaço de ação também dos Estados e da ação tradicional dos Estados a este nível; não é só para o cibercrime, é também para os Estados que fazem ciberespionagem, que podem fazer ações disruptivas, etc." (Mendonça, 2023) (Apêndice 4)

Esta é uma fase marcada, igualmente, pela emergência do cibercrime enquanto atividade económica, em que o dinheiro passou a constituir-se como a principal motivação dos *hackers* para atacar.

"Claramente desde esta década, esta é uma atividade económica florescente e que vem crescendo em massa e, portanto, os problemas de cibersegurança também se colocam a este nível [...]" (Verdelho, 2023) (Apêndice 6)

"Aquilo que temos noção é que os ataques que eram normalmente feitos por autodidatas, [...] em que o dinheiro não era a principal motivação, claramente evoluiu bastante para que o dinheiro passasse a ser a principal motivação. Esses autodidatas [...] quase que se

retiraram, porque têm receio de ser confundidos com este ciberterrorismo, com este cibercrime organizado" (Freitas, 2023) (Apêndice 7)

Importa ressaltar, ainda, nesta fase o ano de 2022 como o mais marcante em termos de persistência e magnitude dos ciberataques em Portugal, sobretudo a entidades de grande relevância para o funcionamento da própria sociedade.

"[...] na Europa nós fomos o terceiro país mais atacado em 2022. [...] Aquilo que nós sabemos é que começou no dia 1 de janeiro, com um grande ataque a um grupo de media e não parou. Pela quantidade de sistemas atacados e por serem muito parecidos uns com os outros, entendemos [...] que alguém iniciou um ataque e divulgou que tinham feito um ataque bem-sucedido a um determinado sistema – que tem uma série de vulnerabilidades – e, a partir daí, vulgarizou-se" (Freitas, 2023) (Apêndice 7)

"Um dos anos que é, de facto, um ano marcante nesta área é 2022. Este ano teve ataques muito mediáticos. Começou, aliás, no dia 2 de janeiro de 2022, com um grande ataque a um grande grupo de comunicação social, que é a Impresa. O ano foi muito profícuo em incidentes muito variados, bastante significativos. Houve 25 grandes incidentes em Portugal, em 2022 [...]" (Marques, 2023) (Apêndice 5)

1.2. Fatores que motivaram o aumento dos ciberataques desde 2020

A definição dos seguintes fatores permite-nos compreender os motivos pelos quais se verificou um aumento significativo de ciberataques, em Portugal, a partir de 2020.

Tabela 16: Fatores que motivaram o aumento dos ciberataques desde 2020

Fatores que motivaram o aumento dos ciberataques desde 2020	**Unidades de registo**
Pandemia de Covid-19	**14**
Guerra Rússia-Ucrânia	**5**
Transformação digital	**8**
Falta de literacia digital	2
Globalização	2
Falta de investimento em cibersegurança	1
Emergência de grupos profissionalizados	**5**
Democratização de acesso a ferramentas e serviços de ciberataque	3

Conversão de crime tradicionalmente *offline* para crime *online*	1
Fraca concorrência de cibercriminosos a atuar no mercado português	1
Tensão geopolítica entre a China e os Estados Unidos	1
Emergência do *ransomware as a service*	1
Aumento da inflação	1

A pandemia de Covid-19 constituiu-se como a única categoria mencionada por todos os entrevistados, registando, simultaneamente, o maior registo – 14 referências. Com início em março de 2020 no território português, a pandemia obrigou ao confinamento social da população, o que se traduziu na transferência da vida laboral no escritório para a casa dos colaboradores. Esta mudança expôs, naturalmente, as organizações a um conjunto maior de vulnerabilidades, levando a um incremento significativo do número de ciberataques, sobretudo em momentos de confinamento social.

> *"[...] a pandemia é, certamente, uma causa. Houve um aumento, na ordem dos 80%, dos incidentes registados pelo Centro Nacional de Cibersegurança em 2020. Teve que ver com a pandemia, sem dúvida. E isso teve que ver, certamente, com o oportunismo do cibercrime relativamente a uma circunstância em que havia mais dependência digital e em que as pessoas estavam mais isoladas"* (Mendonça, 2023) (Apêndice 4)

> *"Mas, de uma forma geral, o que lhe posso dizer é que os ataques, com a pandemia, sofreram um incremento muito significativo. Esse incremento era enaltecido quando entrávamos em lockdown"* (Marques, 2023) (Apêndice 5)

> *"[...] de um momento para o outro, as empresas viram-se obrigadas a estender a sua área de atuação literalmente até à casa do colaborador. Portanto, as pessoas estavam numa rede doméstica, não estavam numa rede corporativa, com menos controlos de segurança implementados, [...] muitas vezes com dispositivos pessoais a serem utilizados para aceder a ativos da organização. [...] Portanto, todo este perímetro de segurança que existia ou que estava mais ou menos delimitado àquilo que era a infraestrutura da organização deixou de existir ou estendeu-se até à casa do colaborador. Naturalmente, isto expôs as organizações a outros vetores de ataque"* (Almeida, 2023) (Apêndice 3)

Não obstante, Freitas (2023) acredita que o tipo de ataque que ocorreu durante a pandemia foi, ainda assim, diferente daquele que se veio a sentir em 2022, apontando a pandemia como o principal motivo de aumento do número de ciberataques nos anos seguintes.

"Quando foi a pandemia e viemos todos para casa, houve algum alarmismo do lado das organizações que se estavam a proteger, isto é, até houve investimento adicional em proteger alguns sistemas e aplicações que passaram agora para a cloud e que estavam expostas e publicadas na Internet. A partir do momento em que houve um regresso à normalidade [...] houve aqui um aliviar da vigilância para esses sistemas… Portanto, eu acho que a pandemia claramente ajudou para este aumento, mas refletiu-se um ano e meio quase depois, sobretudo em 2022" (Freitas, 2023) (Apêndice 7)

A verdade é que a pandemia foi entendida como uma oportunidade de negócio para o cibercrime, assistindo-se a um aproveitamento de uma situação de vulnerabilidade para fazer aumentar o número de ciberataques.

"Por exemplo, assistiu-se a um aumento muito grande da aquisição de domínios relacionados com covid, que depois foram utilizados por atacantes para ações de phishing, criação de malware nos dispositivos, etc." (Almeida, 2023) (Apêndice 3)

"Basta ver que, quando foi a pandemia e nós tínhamos de ter o certificado de covid, apareceram logo sites em português a vender o certificado português. Apareceu uma oportunidade de negócio, automaticamente apareceu alguém a tirar partido disso" (Duro, 2023) (Apêndice 2)

Decorrente, em parte, da situação pandémica, segue-se a transformação digital como um dos fatores que motivou o aumento dos ciberataques desde 2020, contabilizando 8 unidades de registo. De acordo com os entrevistados, a maior incorporação do digital nas organizações aliada ao aumento da dependência digital, sobretudo durante a pandemia, criou um cenário com maiores vulnerabilidades e, portanto, fez disparar o número de ataques em Portugal.

"Claramente que não se pode deixar passar a transição digital a que todos nós fomos obrigados nestes últimos anos. Como é óbvio, houve uma migração de muitos sistemas para a cloud e depois o facto da conectividade passar a ser feita a partir das nossas casas. [...] Claramente esta transição digital foi um grande gatilho para que aumentasse os ciberataques durante a pandemia" (Freitas, 2023) (Apêndice 7)

"Como houve uma aceleração desta transformação digital [com a pandemia], todos os processos foram feitos muito mais rápido, com menos cuidado e, automaticamente, isto criou um conjunto enorme de oportunidades para os cibercriminosos" (Duro, 2023) (Apêndice 2)

Naturalmente, associado a este processo de transformação digital, começa também a emergir o comércio eletrónico, potenciado, uma vez mais, durante a pandemia. Ao fazerem compras *online*, os consumidores estão a expor os seus dados confidenciais na *Internet*, facilitando o seu acesso por parte dos *hackers*.

> *"A pandemia, por exemplo, fez disparar para números astronómicos os valores de comércio eletrónico. E perante este cenário, os cibercriminosos começaram a explorar possibilidades à volta de toda esta atividade de ganhar dinheiro sem ter de fazer grande esforço"* (Verdelho, 2023) (Apêndice 6)

De mencionar, ainda, a guerra entre a Rússia e a Ucrânia e a emergência de grupos profissionalizados como fatores de destaque que motivaram o aumento dos ciberataques desde 2020, ambos com 5 unidades de registo.

Por um lado, os entrevistados acreditam que a guerra na Ucrânia se constituiu como uma oportunidade assente numa situação de vulnerabilidade, naturalmente aproveitada pelos *hackers* para fazer proliferar os seus ataques.

> *"Há uma tensão clara no mundo físico, que se manifestou em guerra com a invasão da Ucrânia pela Rússia e, logo aí, deu origem, direta ou indiretamente, a uma proliferação de ataques [...]"* (Marques, 2023) (Apêndice 5)

> *"A guerra na Ucrânia está a ser usada massivamente para ataques, quer para disseminar armas de ataque a supostos exércitos que deviam ajudar a Ucrânia, mas depois essas armas vão estar a navegar livremente sabe-se lá na mão de quem, quer sites que pedem dinheiro para a Ucrânia e são falsos"* (Duro, 2023) (Apêndice 2)

Por outro lado, começam a emergir grupos profissionalizados de cibercriminosos, com técnicas muito mais sofisticadas e com uma capacidade muito maior de fazer proliferar os seus ataques.

> *"[...] começa-se a assistir também a uma concentração grande de grupos profissionalizados, que fazem este tipo de ataques, seja numa ótica de serviço, ou seja, tu contratares o serviço para fazer determinado ataque, seja numa ótica de ganharem notoriedade e relevância dentro do meio ou para fins financeiros e económicos, e até numa ótica de ativismo"* (Almeida, 2023) (Apêndice 3)

"[...] o cibercrime, os atores estatais, os ativistas e outros vão-se tornando mais sofisticados, vão-se tornando mais profissionalizados e, portanto, aproveitam as oportunidades com mais facilidade" (Mendonça, 2023) (Apêndice 4)

1.3. Atual panorama de ciberataques em Portugal

1.3.1. Tipos de ataque mais frequentes

Tabela 17: Tipos de ataque mais frequentes em Portugal

Tipos de ataque	Unidades de registo
Phishing	**6**
Ransomware	**9**
Fraude	4
Negação de serviço	2
Perda de controlo	4
Perda de dados	**5**
Smishing	1
Vishing	1
Brand phishing	1
Backdoor	1
CEO *fraud*	1

O *ransomware* foi apontado como o tipo de ataque mais frequente, atualmente, em Portugal, contabilizando 9 unidades de registo. Tendo em vista a obtenção de dinheiro, Freitas (2023) sublinha que, em grande parte dos ataques, os *hackers* acedem a informação confidencial da organização para mais facilmente negociar o pagamento do resgate, embora seja da opinião que as organizações nunca devem pagar.

"À cabeça da preocupação temos o ransomware. O ransomware é um ataque muito simples, que passa por mandar um e-mail para alguém, alguém dentro de uma organização abre o e-mail e, se for ransomware moderno, isto tem a potencialidade de bloquear completamente o sistema da empresa" (Verdelho, 2023) (Apêndice 6)

"[...] temos o ransomware, que continua a ser claramente um problema. O ransomware, no passado, era algo que encriptava e pedia dinheiro. Neste momento, já vamos na situação do triple ransomware" (Duro, 2023) (Apêndice 2)

Com um valor correspondente a 6 unidades de registo, segue-se o *phishing* como o segundo tipo de ataque mais frequente, segundo a perspetiva dos entrevistados. Diretamente relacionado com a perda de dados (5 unidades de registo), Duro (2023) sublinha que o *phishing* é apenas um veículo para o ataque, porque aquilo que se obtém do *phishing*, normalmente, são credenciais. Ainda assim, é apontado como um dos ataques mais comuns, atualmente, em Portugal.

> *"Relativamente aos incidentes de cibersegurança, o mais frequente é, sem dúvida, o phishing. Mas não quer dizer que todo o phishing tenha resultados, porque nós registamos o phishing independentemente de ele ter sucesso ou não. [...] o phishing é, sem dúvida, o 'campeão' dos incidentes, que afeta o fator humano, em particular"* (Mendonça, 2023) (Apêndice 4)

> *"Os tipos de ataques mais frequentes tem sido muito a componente do ransomware e do phishing"* (Almeida, 2023) (Apêndice 3)

1.3.2. Setores de atividade mais atacados

Tabela 18: Setores de atividade mais atacados em Portugal

Setores de atividade	Unidades de registo
Saúde	**5**
Educação	**5**
Infraestruturas críticas	2
Administração pública	**4**
Banca	**4**
Corporate	1
Direito	1
Indústria	2
Comércio	1
Serviços digitais	1

De acordo com a perspetiva da maioria dos entrevistados, a saúde e a educação constituem-se como os dois setores de atividade mais atacados, atualmente, em Portugal, ambos com 5 unidades de registo. Duro (2023) explica-nos o porquê de estas serem as áreas onde se registam um maior número de incidentes.

"Porque é que a área da saúde começa aqui a aparecer como área de ataque? Porque se a área da saúde tiver um ataque de ransomware, a probabilidade de pagar é muito grande, porque estão vidas em risco" (Duro, 2023) (Apêndice 2)

"[...] porque é que a área da educação, às vezes, é tão atacada? Porque se for um ambiente mais aberto, mais descontraído, eu posso conseguir um grande número de agentes infetados para, posteriormente, fazer os ataques" (Duro, 2023) (Apêndice 2)

Por sua vez, a administração pública e a banca são igualmente apontadas como dois setores de atividade frequentemente alvo de ciberataques, ambos com 4 unidades de registo.

"Quanto aos setores de atividade, temos a banca, ou seja, os clientes da banca, através do phishing, são muito atacados. A banca em si tem muita maturidade ao nível da cibersegurança, tem uma grande capacidade de defesa e de resposta. Mas os clientes estão mais suscetíveis, digamos" (Mendonça, 2023) (Apêndice 4)

"A banca, naturalmente, é apetecível pelo tipo de negócio que tem [...]" (Almeida, 2023) (Apêndice 3)

"A administração pública também. Nos últimos anos, em particular, as câmaras municipais têm sofrido alguns ataques" (Mendonça, 2023) (Apêndice 4)

1.3.3. Riscos inerentes às organizações mais verificados

Tabela 19: Riscos inerentes às organizações mais verificados em Portugal

Riscos	Unidades de registo
Paralisação temporária de atividade	**4**
Falência de empresas	2
Comprometimento de dados pessoais e confidenciais	**4**
Dano reputacional	1
Quebra financeira	**4**
Pagamento de resgate	**4**
Aplicação de coimas por parte dos reguladores	1

De entre o conjunto de riscos inerentes às organizações mais verificados, atualmente, em Portugal, destacam-se a paralisação temporária de atividade, o comprometimento de dados

pessoais e confidenciais, a quebra financeira e o pagamento de resgate, todos com um valor correspondente a 4 unidades de registo.

> *"Quanto aos riscos, por exemplo, aqueles ataques que ocorreram em 2022 provocaram a indisponibilidade de serviços, quer da própria empresa, quer das empresas por elas servidas"* (Marques, 2023) (Apêndice 5)

> *"Um outro aspeto é a exfiltração de dados, portanto o comprometimento de dados pessoais de clientes, fornecedores e colaboradores e depois como é que esses dados são utilizados pelo cibercrime ou, até, por agentes estatais que queiram utilizar dados com um valor sensível"* (Mendonça, 2023) (Apêndice 4)

> *"Depois, obviamente, o impacto de quebra operacional. Recordo-me que havia uma empresa, há uns anos, que foi atacada, teve dois ou três dias parada por causa de um ataque de ransomware e teve um impacto de cerca de 2 milhões de euros – e falamos, então, do impacto financeiro"* (Almeida, 2023) (Apêndice 3)

> *"Aquilo que realmente assistimos é que houve muitas entidades a pagar [o resgate] porque não tinham tomado medidas que lhes permitisse depois recuperar de forma mais tranquila ou controlada de um ataque de ransomware"* (Freitas, 2023) (Apêndice 7)

1.4. Importância de uma organização segura

Revelou-se necessário compreender a opinião dos entrevistados relativamente à importância de manter uma organização segura, ou seja, o motivo pelo qual as organizações devem implementar políticas de cibersegurança.

Tabela 20: Importância de uma organização segura

Importância de uma organização segura	**Unidades de registo**
Prevenir a ocorrência de ciberataques	**4**
Garantir a capacidade de recuperação de um incidente	**3**
Garantir a segurança dos *stakeholders*	2
Garantir a confiança do mercado	2
Evitar disrupção de serviço	**3**
Evitar quebras operacionais	1
Evitar o pagamento de multas	1
Evitar perda reputacional	1

A maior parte dos entrevistados referiu que é importante manter uma organização segura para prevenir a ocorrência de ciberataques – 4 unidades de registo. Naturalmente, se uma organização apostar em ações e medidas de segurança para se proteger, estará certamente a prevenir sofrer um ciberataque.

> *"Uma organização que aposte na cibersegurança, evidentemente, reduz o risco de sofrer um incidente de cibersegurança. O risco não passa para zero, mas é reduzido, é mitigado"* (Mendonça, 2023) (Apêndice 4)

> *"[...] mais vale prevenir do que remediar, porque, de facto, remediar nem sempre conseguimos, o que quer dizer que temos de antecipar o estrago e antecipar é ter estruturas empresariais de segurança"* (Verdelho, 2023) (Apêndice 6)

Importa mencionar, também, que as organizações devem apostar na cibersegurança para garantir a capacidade de recuperação de um incidente e evitar disrupção de serviço, o que corresponde a um valor de 3 unidades de registo para ambas.

No que respeita à primeira categoria, é realmente importante uma organização ter a capacidade de recuperar do incidente, mesmo que não consiga eliminar a hipótese de sofrer um incidente (Mendonça, 2023). Esta capacidade de recuperação é conseguida através de um nível de maturidade em cibersegurança mais elevado.

> *"As empresas que foram atacadas e que estavam bem preparadas, recuperaram num tempo finito e não perderam informação. Conseguiram recuperar tudo, só não recuperaram o tempo que perderam na fase de recuperação. As outras que não estavam preparadas, ou tão bem preparadas, não só perderam informação para sempre, como não conseguiram recuperar completamente, ou seja, houve sistemas e serviços que não voltaram a ser repostos"* (Marques, 2023) (Apêndice 5)

Relativamente à segunda categoria, Almeida (2023) defende que, numa perspetiva interna, é fundamental a organização estar segura para evitar disrupção de serviço. Isto revela-se ainda mais importante quando se trata de serviços considerados essenciais, cuja sua disrupção poderá provocar grandes comprometimentos no funcionamento da sociedade.

> *"Nós estamos a desmaterializar, estamos a viver num mundo cada vez mais interligado e dependente da Internet e dos sistemas informáticos. Até mesmo sistemas muito básicos, como a água e a eletricidade, dependem de um sistema informático que faz a gestão. [...]*

Se alguém fizer um ataque a um sistema destes, automaticamente podemos não ter água numa cidade durante umas horas muito grandes" (Duro, 2023) (Apêndice 2)

1.5. Maturidade das empresas portuguesas em cibersegurança

Como constatámos anteriormente, o grau de maturidade de uma empresa em matéria de cibersegurança pode determinar a sua capacidade de mitigar e responder a um ciberataque.

Tabela 21: Maturidade das empresas portuguesas em cibersegurança

Maturidade das empresas portuguesas em cibersegurança	**Unidades de registo**
Aumento generalizado do grau de maturidade	**6**
Grau de maturidade ainda insuficiente	3
Grandes empresas com elevado grau de maturidade	4
PME's com reduzido grau de maturidade	**10**

Ao nível da dimensão das organizações, a totalidade dos entrevistados concorda que existe um reduzido grau de maturidade em cibersegurança nas PME's portuguesas, contabilizando 10 unidades de registo. Tratando-se de empresas mais pequenas, à partida com menos capital, é natural que o seu investimento em cibersegurança não seja tão elevado quando comparado com as grandes empresas, estando, por isso, mais propensas a sofrer um ciberataque.

"No caso das [instituições] mais pequenas, [...] por norma, não há sensibilidade para a temática, logo não há orçamento e, automaticamente, não há três coisas que são fundamentais: formação das pessoas, recursos humanos dedicados e com know-how suficiente e, obviamente, recursos tecnológicos para proteger as empresas" (Duro, 2023) (Apêndice 2)

"[...] em termos estatísticos, acho que 60% ou 70% das PME's que são atacadas fecham portas nos 6 meses seguintes. Isto revela logo a fragilidade e a capacidade de resposta de uma PME àquilo que é o ciberataque. Também porque tipicamente têm menos capacidade de investimento em segurança [...]" (Almeida, 2023) (Apêndice 3)

Por conseguinte, estas empresas têm uma maior dificuldade em prevenir e recuperar do incidente, daí a importância de apostarem na cibersegurança.

"Os dados mostram muito que, por exemplo, a grande dificuldade que as PME's têm, em Portugal, é recuperar do incidente, é voltar a colocar os serviços disponíveis para os clientes e para os colaboradores" (Mendonça, 2023) (Apêndice 4)

Do ponto de vista global, importa destacar o aumento generalizado do grau de maturidade das empresas portuguesas em cibersegurança, com um valor correspondente a 6 unidades de registo. Embora os entrevistados concordem que as PME's ainda têm um grau de maturidade insuficiente, a verdade é que se tem verificado um aumento generalizado da consciência das organizações portuguesas no que respeita à importância da implementação de políticas de cibersegurança.

"Tem havido um grau de maturidade que está a crescer consideravelmente. A cibersegurança já é um tópico discutido a nível dos conselhos de administração, já existe essa sensibilização. O risco cibernético já é considerado em muitas organizações e tratado como um risco operacional. Portanto, esse nível de consciencialização e de sensibilização tem aumentado bastante, o que é muito positivo" (Almeida, 2023) (Apêndice 3)

"[...] as organizações, em geral, têm agido de uma forma muito positiva. [...] Ao nível das políticas públicas e a nível institucional, nós estamos muito bem classificados a nível internacional" (Mendonça, 2023) (Apêndice 4)

"[...] eu acho que há consciência. Do ponto de vista de awareness, tem havido um aumento crescente nas organizações" (Freitas, 2023) (Apêndice 7)

Ainda assim, Freitas (2023) sublinha que, apesar da evolução positiva, o grau de maturidade das empresas portuguesas em cibersegurança ainda é insuficiente.

"Nota-se uma melhoria, mas continua a ser fraco. Se tivesse de colocar numa escala de 1 a 10, diria que o grau de preparação é entre um 4,5 e um 5. Saiu de muito fraco para um médio fraco" (Freitas, 2023) (Apêndice 7)

1.6. Medidas de segurança

É sabido que, em situação de ciberataque, se deve adotar essencialmente uma atitude preventiva. Esta atitude passa pela implementação de ações e medidas de segurança que ajudem as organizações a proteger-se de eventuais ataques, daí a importância de estarem consciencializadas acerca das melhores práticas.

Tabela 22: Medidas de segurança

Medidas de segurança	Unidades de registo
Formação dos colaboradores	**17**
Aplicação de processos regulatórios e orientadores	4
Realização de avaliações de risco	**7**
Estabelecimento de procedimentos de *backup* Seguros	**7**
Gestão de identidades e acessos	**10**
Investimento em tecnologia	**8**
Monitorização de eventuais ataques ou ações de atividades de risco	1
Contratação de pessoas com formação adequada na área da cibersegurança	2
Definição de uma equipa de operações de segurança	3
Definição de um plano de recuperação	3
Definição de um plano estratégico de segurança	2
Definição da informação crítica, confidencial e pública	2
Identificação de funções ou atividades críticas	2
Segmentação das redes	2
Avaliação da rede convencional	1
Definição de uma estratégia de testagem regular	**6**
Estabelecimento de atualizações de segurança regulares	3
Inventariação dos ativos que constituem os sistemas de informação	2
Definição de uma política de utilização dos recursos TIC	1
Estabelecimento de um registo histórico centralizado	1

De entre o conjunto de medidas de segurança apresentado na Tabela 22, compreende-se que a formação dos colaboradores é a medida mais vezes mencionada pelos entrevistados, contabilizando 17 unidades de registo. Segundo Verdelho (2023), cerca de 90% dos problemas de cibersegurança são problemas humanos. Por esse motivo, revela-se cada vez mais necessário as organizações desenvolverem ações de formação e consciencialização em cibersegurança junto dos seus colaboradores, de forma permanente e constante.

"[...] independentemente do valor que as empresas invistam em soluções tecnológicas e que eventualmente forcem as ações ou os comportamentos dos colaboradores, a pessoa há de ser sempre a primeira linha de ataque ou a primeira linha de defesa, dependendo do quão sensibilizada estiver ou não para a cibersegurança. [...] Para que as pessoas mudem um bocado os seus comportamentos, é importante que sejamos capazes de mudar as suas convicções e que percebam qual é o impacto desses seus comportamentos, quer para a sociedade, quer para a organização. Portanto, eu diria que é fundamental esta componente de sensibilização" (Almeida, 2023) (Apêndice 3)

"[...] as pessoas têm de ser formadas e tem de se escolher uma cultura de continuidade, ou seja, a cibersegurança não pode ser uma ação de formação que se tem uma vez por ano, aquela coisa chata das passwords. Tem de ser uma cultura instalada" (Mendonça, 2023) (Apêndice 4)

"[...] é essencial fazermos essas formações e essas ações, mas eu diria que deveríamos ir mais além, que é educar os colaboradores com ações permanentes" (Duro, 2023) (Apêndice 2)

Os colaboradores têm de estar de tal forma consciencializados para a temática que compreendam o valor fundamental dos seus comportamentos e ações para a proteção de toda a organização, desempenhando um papel ativo na prevenção e mitigação de ciberataques. Segundo alguns entrevistados, esta mudança de mentalidade só é possível através de formas criativas e interessantes de passar a mensagem, para que os colaboradores assimilem efetivamente a informação que lhes está a ser transmitida.

"Um dos investimentos que as organizações têm de fazer – e até o nosso papel como IBM – é tornar as formações interessantes, desejáveis, para que os colaboradores desejam ter mais informações do género, porque acrescentam valor, porque se sentem mais seguros e sentem que estão a tornar a organização mais segura. Essa sensação de valor tem de ser cada vez mais bem passada para o colaborador. [...] por isso, sim awareness, sim formação, mas formação não só sobre o que é a ameaça, mas como é que eles podem fazer parte da solução" (Freitas, 2023) (Apêndice 7)

"Faz parte já das políticas de um grande número de organizações haver esta sensibilização dos colaboradores, mas, muitas das vezes, ela é feita de forma uniforme a toda a organização, sem grande distinção entre o indivíduo [...] Mas isto tem uma limitação muito grande que é as pessoas não assimilam os conteúdos e não há engagement

das pessoas para com esta informação. Portanto, é fundamental ter formas criativas e diferentes de passar esta mensagem aos colaboradores" (Almeida, 2023) (Apêndice 3)

"Educando as pessoas, automaticamente reduzimos o risco, se calhar de uma forma drástica. [...] Por isso, é muito importante que as pessoas colaborem e participem na segurança, não colocando à prova os sistemas de cibersegurança" (Duro, 2023) (Apêndice 2)

Esta é uma questão de elevada importância, inclusive, para as entidades com autoridade em matéria de cibersegurança, estando já em prática algumas medidas e ações que promovem a formação dos colaboradores.

"[...] a Estratégia Nacional de Segurança do Ciberespaço, aquela que ainda está em vigor, tem um eixo que é o eixo 2, da capacitação, onde a maior parte das iniciativas dos diversos planos de ação que temos tido ao longo da vigência da estratégia estão na capacitação das pessoas, a começar pela sensibilização, alertando para os problemas. No CNCS, temos também a iniciativa C-Academy, que visa formar 9800 profissionais de cibersegurança até 2026, através de uma rede de todos os politécnicos e universidades públicas do nosso país" (Marques, 2023) (Apêndice 5)

Segue-se a gestão de identidades e acessos como uma medida de segurança a implementar nas organizações, registando 10 referências.

"[...] gestão de identidades e acessos e gestão privilegiada de acessos é mesmo muito importante. Isto é uma componente muito importante do zero trust e vou-lhe dizer que, em muitos dos ataques a que respondemos o ano passado, um dos problemas foi que, ao apoderarem-se do sistema, conseguiram muito facilmente escalar privilégios de utilizadores" (Freitas, 2023) (Apêndice 7)

Por conseguinte, os entrevistados mencionaram duas medidas essenciais que se enquadram numa política de gestão de identidades e acessos: definição de *passwords* fortes e ativação do múltiplo fator de autenticação. A implementação destas medidas ajudará as organizações a proteger não só os seus recursos, como também os seus colaboradores.

"É importante também ter uma correta gestão e controlo de identidades e acessos, como, por exemplo, políticas de passwords fortes, ter mecanismos de multi-factor authentication…" (Almeida, 2023) (Apêndice 3)

"Deve-se ter uma autenticação múltiplo fator, não se deve autenticar só com username e password, porque, através de mecanismos de phishing, essas credenciais são exfiltradas e depois são utilizadas por quem quer fazer mal para entrar na nossa conta" (Marques, 2023) (Apêndice 5)

O investimento em tecnologia constitui-se como outra medida de segurança considerada importante pelos entrevistados, contabilizando 8 unidades de registo. Investir em estruturas tecnológicas permite não só prevenir a ocorrência de ciberataques, como também recuperar de forma mais eficaz do incidente.

"É importante que as empresas se dotem dos controlos de segurança que são necessários para tentar antecipar e identificar um possível ataque, agir e conter esse ataque e recuperar de um ciberataque" (Almeida, 2023) (Apêndice 3)

"Ter estruturas tecnológicas, ou seja, ter montado nas empresas a tecnologia de segurança necessária, entre firewalls, anti-malware, coisas dessa natureza" (Verdelho, 2023) (Apêndice 6)

"E, por último, obviamente, ter tecnologia adequada e não se comprar a falsa sensação de segurança" (Duro, 2023) (Apêndice 2)

Com um registo de referências igualitário (7 unidades de registo), os entrevistados também referiram a realização de avaliações de risco e o estabelecimento de procedimentos de *backup* seguros como medidas de segurança a implementar nas organizações.

Por um lado, a realização de avaliações de risco é fundamental para identificar os riscos e, posteriormente, conseguir detê-los. Além de uma identificação clara do risco, é necessário quantificá-lo, para poder justificar à organização todos os investimentos realizados em cibersegurança.

"Devem fazer uma correta avaliação de risco, precisamente para perceberem qual é o risco a que estão expostas e perceberem quais são os ativos sobre os quais têm de agir" (Almeida, 2023) (Apêndice 3)

"Devem fazer análises de risco relativamente a esses dados críticos e às ameaças que, normalmente, afetam essa organização, para depois priorizar aquilo que é importante e aquilo que não é importante" (Mendonça, 2023) (Apêndice 4)

"Uma das mensagens mais importantes que eu tenho é: quantifiquem o risco. [...] Eu acho que assim é muito mais fácil um chief information security officer suportar a razão pela qual temos de fazer este investimento e temos de ter um plano estratégico, que tem de ser cumprido rigorosamente" (Freitas, 2023) (Apêndice 7)

Por outro lado, é necessário estabelecer procedimentos de *backup* seguros, para garantir uma maior segurança e proteção da informação organizacional, sobretudo a informação crítica e confidencial.

"Terem um mecanismo de backups seguros, portanto segregados daquilo que é a rede principal, que não permitam também a adulteração ou que sejam comprometidos através de um determinado tipo de ataque" (Almeida, 2023) (Apêndice 3)

"Devem ter backups da informação mais crítica, é essencial" (Mendonça, 2023) (Apêndice 4)

"Outra medida é os backups estarem offlines [...]" (Marques, 2023) (Apêndice 5)

Importa destacar, ainda, a definição de uma estratégia de testagem regular, com um valor correspondente a 6 unidades de registo. Segundo os entrevistados, não basta apenas as organizações investirem em tecnologia, definirem planos estratégicos e apostarem na formação dos colaboradores, é essencial testá-los.

"[...] tem que se testar as pessoas e as tecnologias [...]" (Mendonça, 2023) (Apêndice 4)

"Eu vou-lhe dizer, grande parte das organizações que foram atacadas tinham planos de segurança, tinham uma maturidade acima da média… Mas nunca testaram os planos de resposta. Portanto, envolver também os colaboradores na parte da testagem, para eles terem consciência de que têm um papel a desempenhar na proteção da organização" (Freitas, 2023) (Apêndice 7)

Sob uma perspetiva diferente, Marques (2023) defende que as organizações devem ter testes de penetração regulares, ou seja, contratar *hackers* benignos que fazem ataques para ver que vulnerabilidades é que a organização tem (Apêndice 5).

1.7. Principais tendências na área da cibersegurança

A cibersegurança tem vindo a ser influenciada por algumas tendências, sobretudo ao nível das tecnologias emergentes, pelo que se revela pertinente compreender quais as tendências que estão a ter um maior impacto na área.

Tabela 23: Principais tendências na área da cibersegurança

Tendências	Unidades de registo
Inteligência Artificial	**11**
5G	**6**
Internet of Things	**6**
Cloud computing	3
Computação quântica	**7**
Edge computing	1
Globalização	1

No topo das principais tendências na área da cibersegurança mencionadas pelos entrevistados encontra-se a Inteligência Artificial, com 11 unidades de registo. Os entrevistados acreditam que os ciberataques começam a ser cada vez mais sofisticados e, consequentemente, difíceis de mitigar devido à incorporação de Inteligência Artificial.

> *"[...] estou convencido de que os ciberataques vão começar a ser cada vez mais estimulados pela Inteligência Artificial utilizada para fins maliciosos"* (Marques, 2023) (Apêndice 5)

> *"Neste momento, estamos preocupados e temos feito cada vez mais ações de consciencialização dos nossos clientes em termos de Inteligência Artificial, que pode ser realmente uma ameaça. Por isso, fazer avaliações de qual é a nossa exposição a tecnologias baseadas em Inteligência Artificial começa a ser cada vez mais importante"* (Freitas, 2023) (Apêndice 7)

> *"[...] pode estar a emergir uma tendência que também deve ser considerada que é a Inteligência Artificial, que facilita o acesso de terceiros, não especializados, a instrumentos para realizar ações maliciosas no ciberespaço, como desinformação ou, mesmo até, programas maliciosos"* (Mendonça, 2023) (Apêndice 4)

A computação quântica é outra das tendências na área da cibersegurança várias vezes apontada pelos entrevistados, contabilizando 7 unidades de registo. À semelhança da Inteligência Artificial, os entrevistados mostram-se preocupados com a utilização da computação quântica para fins maliciosos.

> *"A cibersegurança está muito assente naquilo que são os algoritmos e as técnicas criptográficas atuais, por isso tem existido sempre uma evolução em termos da dimensão*

das chaves e dos algoritmos que são utilizados… Mas todos eles se baseiam na premissa de que, num tempo considerado seguro, não é possível replicar aquela função criptográfica ou quebrar aquela cifra. Com a computação quântica, os algoritmos existentes podem, com relativa frequência, ser quebrados por utilização de computação quântica numa janela temporal que já não é considerada segura" (Almeida, 2023) (Apêndice 3)

"[...] a IBM é pioneira na computação quântica e, neste momento, também estamos muito preocupados com o impacto que a computação quântica poderá ter, por exemplo, nas chaves criptográficas. Nós sabemos que, hoje em dia, há chaves criptográficas que poderão demorar 5 mil anos a ser decifradas, mas com o aumento da capacidade de processamento dos cúbitos da computação quântica possa ser reduzido para 3 ou 4 dias" (Freitas, 2023) (Apêndice 7)

Os entrevistados fizeram questão de destacar, ainda, o 5G e a *Internet of Things* como tendências na área da cibersegurança, ambos com 6 unidades de registo.

Com um aumento significativo de banda larga, os entrevistados acreditam que o 5G poderá fazer aumentar a proliferação de ciberataques, por permitir uma maior interligação entre dispositivos.

"Começo por falar do 5G. Se olharmos para aquilo que foi a transformação digital que houve com a evolução para o 3G e depois para o 4G, estamos a falar de um aumento de banda larga brutal e, para o 5G, irá acontecer a mesma coisa. Portanto, isto vai permitir que haja muito mais dispositivos interligados, muito mais comunicação entre estes dispositivos e, portanto, vai permitir, naturalmente, criar novos vetores de ataque para os quais ainda não estaremos totalmente preparados" (Almeida, 2023) (Apêndice 3)

No caso da *Internet of Things*, os entrevistados manifestam igualmente a sua preocupação, na medida em que se irá assistir a um aumento significativo das superfícies de ataque que, por sua vez, facilitará a proliferação dos ciberataques.

"Isto vai fazer com que apareçam uma série de dispositivos que, provavelmente, até hoje estavam escondidos, como câmaras, como sensores, como portões, como lâmpadas… aqueles dispositivos do IoT que estão todos interligados e que vão aumentar brutalmente as tais superfícies de ataque e, consequentemente, os vetores de ataque. Esta é outra preocupação que vai acontecer no futuro" (Duro, 2023) (Apêndice 2)

"[...] trazem novas vulnerabilidades, novas camadas de complexidade, mais sofisticação aos ciberataques e aumentam a superfície de ataque, como é o caso da Internet of Things" (Mendonça, 2023) (Apêndice 4)

1.8. Principais desafios na área da cibersegurança

Sendo a cibersegurança uma área tão complexa, revela-se necessário compreender os desafios inerentes à sua atuação.

Tabela 24: Principais desafios na área da cibersegurança

Desafios	Unidades de registo
Falta de cultura de cibersegurança nas organizações	**8**
Fator humano	**11**
Falta de recursos	4
Complexidade dos ciberataques	**9**
Tecnologias emergentes	**8**
Redefinição mais sofisticada de *malwares* já existentes	2
Falta de atualizações de segurança	3
Falta de *security by design* nas aplicações e sistemas	2
Democratização de acesso a ferramentas e serviços de ciberataque	1
Dificuldade em justificar os investimentos em cibersegurança nas organizações	1
Migração para a *cloud*	2
Acompanhamento da tendência regulatória da União Europeia	1

Na perspetiva dos entrevistados, o principal desafio na área da cibersegurança é o fator humano, com um valor correspondente a 11 unidades de registo. Como já foi referido anteriormente, a grande maioria dos problemas de cibersegurança é provocada por falhas humanas, na maior parte das vezes não intencionais, que acabam por comprometer a própria organização.

"Existe aquele clichê de que a pessoa é o elo mais fraco, mas efetivamente continua a ser. Porque se a pessoa não clicar naquele link, se não for àquele site, se não usar o recurso da empresa de forma indevida, vamos testar menos a firewall ou o antivírus. Vai existir

menos testes e diminui claramente a probabilidade de uma empresa ser atacada" (Duro, 2023) (Apêndice 2)

"[...] muitos destes incidentes que conduzem a um grande impacto, que têm que ver com ransomware, também começam com o fator humano. Ou seja, alguém que clica onde não deve, alguém que partilha uma password com quem não deve ou até alguém que autoriza, sem querer, o acesso de terceiros a uma conta privilegiada, por exemplo, através do múltiplo fator de autenticação que, às vezes, não é suficientemente seguro, porque as pessoas autorizam quando não devem" (Mendonça, 2023) (Apêndice 4)

"O problema é que numa organização de 200 pessoas, basta que uma faça clique num link errado para comprometer toda a organização" (Marques, 2023) (Apêndice 5)

Segue-se um segundo desafio relacionado com a complexidade dos ciberataques, registando 9 referências realizadas pelos entrevistados. A verdade é que os ciberataques têm-se tornado cada vez mais difíceis de defender e mitigar, devido à utilização de ferramentas mais sofisticadas e complexas, tornando-se um grande desafio para as organizações conseguirem prevenir a sua ocorrência.

"[...] a complexidade e a criatividade dos ataques, ou seja, eles têm-se tornado cada vez mais complexos de se defender, de detetar e de mitigar, também pela panóplia de ferramentas, de soluções tecnológicas e da própria evolução tecnológica, que está não só à disposição de quem está a defender as organizações, como também de quem as está a atacar" (Almeida, 2023) (Apêndice 3)

"Deixe-me dizer-lhe também uma grande evolução nos ataques que diz respeito à velocidade com que eles conseguem tornar um ataque eficaz. Isto é, muitas vezes, chegávamos a estar 240 e poucos dias desde o primeiro contacto até que o atacante conseguisse ser eficaz. Hoje em dia, pode ser realizado facilmente em 72 horas" (Freitas, 2023) (Apêndice 7)

"A complexidade é um dos grandes desafios da cibersegurança" (Mendonça, 2023) (Apêndice 4)

Os entrevistados mencionaram, ainda, com algum destaque, a falta de cultura de cibersegurança nas organizações e as tecnologias emergentes como desafios a enfrentar na área da cibersegurança, ambos com 8 unidades de registo.

No que se refere à falta de cultura de cibersegurança nas organizações, os entrevistados argumentam que a falta de investimento em cibersegurança, seja através da implementação de tecnologia, seja através da capacitação dos trabalhadores, se constitui como um desafio na área da cibersegurança.

> *"Há aqui duas questões na cibersegurança: primeiro, é se tecnologicamente há evolução ou não e isso é um desafio; segundo, é as empresas assumirem que têm de investir e que têm de levar este tema a sério"* (Duro, 2023) (Apêndice 2)

> *"[...] acho que algumas organizações ainda têm dificuldade em perceber como é que devem fazer o seu investimento em cibersegurança e por onde é que devem evoluir. Isto porque o mercado em cibersegurança tornou-se muito apetecível nos últimos anos, para quem faz essa venda de serviços, produtos, soluções… E, portanto, como esta oferta começa a ser tão grande, às vezes as organizações sentem-se um bocado exacerbadas, no sentido em que têm alguma dificuldade em perceber o que devem contratar, onde devem contratar, que serviços devem ou não implementar"* (Almeida, 2023) (Apêndice 3)

Relativamente às tecnologias emergentes, como mencionado anteriormente, estas têm vindo a constituir-se como um grande desafio para as organizações, sobretudo interligadas a ferramentas cada vez mais complexas de ataque. O avanço de tecnologias como a Inteligência Artificial, o 5G, a *Internet of Things*, a computação quântica ou a *cloud computing* poderá trazer uma dificuldade acrescida em termos de deteção, prevenção e recuperação de um ciberataque.

> *"A globalização e a cloud continuam, inevitavelmente, a ser um desafio muito grande. Porque a cloud é algo muito novo, que está a evoluir a uma velocidade muito grande e, às vezes, não há recursos suficientes para acompanhar essa evolução. Por exemplo, há recursos de quem desenvolve a cloud, mas não há recursos depois de quem é cliente e vive da própria cloud. E isto vai continuar a gerar desafios. [...] Quando tivermos o 5G efetivamente em todo o seu potencial, então vamos ter aí também um grande desafio, porque é quando tudo se interligar com tudo e, muito provavelmente, deixarmos de usar as redes tradicionais"* (Duro, 2023) (Apêndice 2)

> *"A Inteligência Artificial também, obviamente, porque começa a haver esta democratização e estar ao acesso de todos. Acho que vai ser um game changer também, porque é uma solução tecnológica que está também à disposição dos atacantes"* (Almeida, 2023) (Apêndice 3)

1.9. Futuro dos ciberataques em Portugal

Compreender o futuro dos ciberataques em Portugal poderá ser uma mais-valia para conseguir antecipar eventuais ameaças que poderão ocorrer e, a partir daí, adotar as políticas mais adequadas de prevenção de eventuais ataques.

Tabela 25: Futuro dos ciberataques em Portugal

Futuro dos ciberataques em Portugal	Unidades de registo
Aumento significativo do número de ciberataques	**3**
Maior sofisticação	**4**
Maior influência das tecnologias emergentes	**14**
Aumento da sensação de ameaça	2
Aumento da capacidade de mitigação e recuperação de ciberataques	2
Aumento da literacia digital	1
Emergência das ameaças híbridas	2
Maior convergência entre ciberterrorismo e cibercrime	1
Emergência da ciberguerra	**3**

De acordo com os entrevistados, a maior influência das tecnologias emergentes caracteriza, em larga medida, aquilo que será o futuro dos ciberataques em Portugal, correspondendo a um valor de 14 unidades de registo. As tecnologias emergentes não só são uma tendência atual, como irão ter um impacto acrescido no futuro dos ciberataques, devido à sua evolução constante.

> *"O futuro é muito difícil de prever, mas vamos continuar a ver o ransomware, o phishing, vamos começar a ver a Inteligência Artificial cada vez mais nos ciberataques – e isso é uma preocupação –, vamos começar a ver computação quântica, quando ela for desenvolvida a sério e envolvida nos ciberataques – também é uma preocupação"* (Duro, 2023) (Apêndice 2)

> *"Já lhe falei da computação quântica e acho que poderá ser um instrumento para aumentar essa sensação de ameaça. [O futuro] vai passar, também, pela Inteligência Artificial. [...] posso referir também a Internet of Things, que claramente vai massificar e tornar-se um risco"* (Freitas, 2023) (Apêndice 7)

"[...] estou convencido de que a tendência futura vai ser na sofisticação de ataques por via do recurso a algoritmos de Inteligência Artificial" (Marques, 2023) (Apêndice 5)

Diretamente relacionado com a tendência anterior, os entrevistados referem que o futuro dos ciberataques passará, também, por uma maior sofisticação das técnicas e ferramentas utilizadas, com um valor correspondente a 4 unidades de registo.

"[...] acho que os ciberataques vão-se tornar cada vez mais criativos e avançados tecnologicamente [...]" (Almeida, 2023) (Apêndice 3)

"[...] ataques mais sofisticados, isso dá-me a ideia de que vai ser uma tendência, quanto mais não seja porque a tecnologia também está a evoluir e uma coisa está sempre associada à outra" (Marques, 2023) (Apêndice 5)

"A maior sofisticação dos ciberataques, [...] em que cada vez mais se vai cruzar a dimensão técnica do ciberataque com a perceção humana [...]" (Mendonça, 2023) (Apêndice 4)

Com um valor de referências igualitário (3), os entrevistados mencionaram, ainda, o aumento significativo do número de ciberataques e a emergência da ciberguerra para caracterizar o futuro dos ciberataques.

O aumento significativo do número de ciberataques é uma consequência natural da globalização que testemunhamos atualmente e da própria evolução da tecnologia, que permite investir em ferramentas mais sofisticadas e com uma maior capacidade de eficácia.

"Obviamente, o que vamos assistir é a um aumento significativo dos ciberataques. Principalmente, enquanto não conseguirmos ter uma evolução clara da cibersegurança" (Duro, 2023) (Apêndice 2)

"Continua a haver cada vez mais digitalização e, enquanto houver digitalização, continua a crescer o número de pessoas que quer ganhar dinheiro à custa destas atividades. Portanto, quanto mais pessoas houver a circular nas redes, mais serviços digitais há, mais dispositivos há, portanto mais incidentes podem potencialmente ocorrer" (Verdelho, 2023) (Apêndice 6)

A emergência da ciberguerra é uma tendência que conseguimos naturalmente prever, na medida em que o ciberespaço vem facilitar os mecanismos de conflito entre nações que se encontram geograficamente distantes.

"[...] para se falar no futuro, temos de olhar para todos estes atores dos ciberataques e perceber que oportunidades novas cada um deles vai ter. Por exemplo, a cloud pode ser utilizada por uma nação para atacar outra. Porque não? [...] Vamos supor um caso extremo. As nossas empresas de serviços começam todas a meter na cloud os sistemas de gestão que são essenciais para que tudo funcione e esses sistemas de gestão são feitos por um prestador de serviços que não é nacional – e os principais prestadores de serviços não são nacionais. Vamos supor que um dia, por algum motivo, nos chateamos com o país onde está esse prestador de serviço. O que é que impede esse país de cortar o acesso à cloud dos nossos sistemas? Nada. Portanto, está aqui uma oportunidade de um país, no futuro, fazer um ciberataque a outro país" (Duro, 2023) (Apêndice 2)

1.10. Comunicação numa situação de ciberataque

Embora não seja a sua área de atuação, revelou-se pertinente analisar os resultados relativos à perspetiva dos profissionais de Cibersegurança sobre o tema da comunicação, em especial pelo facto de abordarem um caso interessante do ponto de vista da comunicação. A maioria dos entrevistados mencionou a Vodafone como um exemplo no que toca ao papel da comunicação numa situação de ciberataque, enaltecendo a sua gestão de crise como fator determinante para a recuperação do incidente e para a manutenção da reputação organizacional.

"Em particular, o ataque à Vodafone, que teve na comunicação um elemento essencial e eu acho que a generalidade da comunidade percebe que a comunicação foi muito bem gerida, permitindo-lhes uma maior capacidade de recuperar" (Verdelho, 2023) (Apêndice 6)

"[...] já há casos – há um muito conhecido, que foi o da Vodafone – onde a comunicação transparente e contínua foi crítica para que a reputação fosse muito menos afetada" (Freitas, 2023) (Apêndice 7)

"[...] a Vodafone esteve com os serviços indisponíveis durante cerca de 8 dias e isso teve um impacto significativo na performance da empresa. Felizmente, não teve impacto na cotação bolsista, porque eles geriram muito bem o incidente, conseguiram recuperar, conseguiram restabelecer a confiança dos seus clientes. Há um tempo, eu vi a diretora de marketing da Vodafone falar do incidente e percebi que não houve clientes que tivessem mudado a Vodafone para outro provider por causa do incidente, porque, na verdade, eles geriram muito bem" (Marques, 2023) (Apêndice 5)

a) Importância da comunicação

Tabela 26: Importância da comunicação segundo os profissionais de Cibersegurança

Importância da comunicação	Unidades de registo
Informar e esclarecer os *stakeholders*	**5**
Garantir uma maior capacidade de recuperação do incidente	1
Garantir a confiança dos *stakeholders*	1
Tranquilizar os *stakeholders*	1
Proteger a reputação organizacional	1
Garantir uma maior sensação de segurança aos *Stakeholders*	1

Ainda que nem todos os entrevistados tenham manifestado a sua opinião relativamente à importância da comunicação em situação de ciberataque, metade concordou que a comunicação é fundamental para informar e esclarecer os *stakeholders* sobre o incidente e a sua evolução ao longo do tempo, com um valor correspondente a 5 unidades de registo. Significa isto que, se as organizações não apostarem em medidas e ações de comunicação para responder ao incidente, os *stakeholders* dificilmente terão conhecimento sobre a situação e, em alguns casos, não poderão desempenhar o seu papel na resolução do problema.

> *"É importante informar e comunicar com os vários stakeholders [...]"* (Mendonça, 2023) (Apêndice 4)
>
> *"Depois com o público em geral, é importante informar sobre o que está a acontecer, ou seja, eu acho que toda a informação que não prejudique uma investigação ou a recuperação, eu acho que deve ser divulgada"* (Freitas, 2023) (Apêndice 7)

b) Medidas de comunicação

Tabela 27: Medidas de comunicação segundo os profissionais de Cibersegurança

Medidas de comunicação	Unidades de registo
Confirmação da ocorrência do ciberataque	3
Divulgação da situação às autoridades	1
Estabelecimento de um plano de comunicação	2
Definição de um gabinete de crise	1
Comunicação, em tempo real, sobre o que está a	2

Acontecer	
Utilização de uma comunicação factual e transparente	**7**
Utilização de uma comunicação cuidada	**6**
Adoção de uma comunicação interorganizacional	1
Divulgação de boas práticas de cibersegurança	1

Em termos de medidas de comunicação a implementar por uma organização numa situação de ciberataque, verifica-se um consenso de perspetivas entre os entrevistados no que respeita à forma de comunicar.

Por um lado, a maioria dos entrevistados concorda que as organizações devem utilizar uma comunicação factual e transparente, registando um valor correspondente a 7 referências. Por forma a elucidar e esclarecer os *stakeholders* sobre o incidente, revela-se necessário adotar uma comunicação verdadeira, clara e sem margem para dúvidas, em detrimento de optar pelo silêncio ou pela mentira.

> *"[...] por um lado, eu acho que é muito importante comunicar-se rápido e de forma clara [...]"* (Freitas, 2023) (Apêndice 7)

> *"Comparando outros ataques que não foram claros os motivos da comunicação versus aquilo que foi feito no caso da Vodafone, eu vejo, por exemplo, que nos sentimos todos se calhar mais seguros, porque eles assumiram o ataque e foram claros na sua comunicação. Principalmente quando é uma empresa que presta este tipo de serviços e que tem outros a depender desses serviços, uma comunicação que seja assertiva e clara também tira pressão de cima das próprias equipas que estão a trabalhar, porque dá-lhes mais paz de espírito para desenvolver o trabalho"* (Duro, 2023) (Apêndice 2)

Por outro lado, os entrevistados partilham da opinião de que é necessário utilizar uma comunicação cuidada, com 6 unidades de registo. Embora seja importante informar e esclarecer os *stakeholders*, é ainda mais importante selecionar a informação que deve ser ou não partilhada, seja por não existir certezas acerca da sua veracidade, seja por poder comprometer a própria organização.

> *"[...] comunicar com cuidado – ou seja, não dizer aquilo que não se sabe [...]"* (Mendonça, 2023) (Apêndice 4)

> *"Relativamente ao detalhe e à origem, tem de se ter muito cuidado com aquilo que se divulga, até porque, muitas vezes, não sabemos quem é que executou esse ataque e até*

podemos estar a dar informação a pessoas ou entidades que estão envolvidas no próprio ataque. Portanto, também é preciso perceber muito bem a quem é que vamos divulgar essa informação" (Freitas, 2023) (Apêndice 7)

2. O estudo da Comunicação de Crise em situação de ciberataque

Considerando o conjunto de dimensões em estudo, é possível verificar que a categoria referente às medidas de comunicação em situação de ciberataque se destaca, em larga medida, das restantes, registando um valor correspondente a 95 referências. De realçar, ainda, as categorias referentes à situação de crise enfrentada pela empresa alvo de um ciberataque e aos desafios enfrentados pelo profissional de Relações Públicas numa situação de ciberataque, com valores correspondentes a 58 e 48 unidades de registo, respetivamente. Estes destaques podem ser naturalmente justificados pelo maior número de subcategorias que constituem estas dimensões.

Tabela 28: Categorias de análise do conjunto de entrevistas realizadas aos profissionais de Relações Públicas

Categorias	Unidades de recorte
Situação de crise enfrentada pela empresa alvo de um ciberataque	**58**
Importância da comunicação de crise numa situação de ciberataque	35
Papel do profissional de Relações Públicas numa situação de ciberataque	34
Desafios enfrentados pelo profissional de Relações Públicas numa situação de ciberataque	**48**
Medidas de comunicação em situação de ciberataque	**95**
Importância dos *stakeholders* em situação de ciberataque	10
Implicações do ciberataque na reputação organizacional	18
Implicações do fenómeno de ciberataque na área das Relações Públicas	13

2.1. Situação de crise enfrentada pela empresa alvo de um ciberataque

2.1.1. Modo atuação

Para melhor compreender a situação de crise enfrentada pelas organizações entrevistadas, revela-se necessário averiguar o modo de atuação da organização perante o ciberataque, sobretudo ao nível da comunicação.

Tabela 29: Modo de atuação das organizações perante o ciberataque

Modo de atuação	**Unidades de registo**
Informar as autoridades sobre a ocorrência do ciberataque	5
Garantir a articulação entre os vários departamentos internos da organização	**7**
Informar os *stakeholders* sobre o incidente	**8**
Esclarecer os colaboradores sobre o incidente	5
Utilizar uma comunicação factual e transparente	3
Utilizar diferentes canais de comunicação para transmitir a mensagem	3
Controlar a pressão mediática	3
Avaliar a extensão do ciberataque	**7**
Convocar reuniões com diferentes *stakeholders*	1
Responder a entrevistas para os *media*	1

O modo de atuação das organizações entrevistadas perante o ciberataque passou, com um maior destaque, pelas seguintes ações: informar os *stakeholders* sobre o incidente, garantir a articulação entre os vários departamentos internos da organização e avaliar a extensão do ciberataque.

Com um ligeiro destaque, os entrevistados informaram os *stakeholders* sobre a ocorrência do ciberataque, com um valor correspondente a 8 unidades de registo. Informar os *stakeholders* implica mantê-los elucidados acerca da situação, responder às suas dúvidas e tranquilizá-los relativamente à situação.

> *"O nosso maior objetivo – para além de repor a normalidade da operação – era responder objetivamente às questões e inquietações de todos os stakeholders. A nossa estratégia passou por conseguirmos ter todos os stakeholders elucidados"* (Correia, 2023) (Apêndice 9)

"Quando percebemos o que é que tinha sido afetado, houve um grande esforço para se conseguir chegar ao máximo possível de clientes, fornecedores, entidades oficiais – aquelas que eram necessárias" (Simões, 2023) (Apêndice 13)

"Depois de termos conhecimento da extensão dos danos, houve a necessidade de comunicar isso à população e assegurar que a atividade do INEM [...] não tinha sido comprometida" (Borges, 2023) (Apêndice 11)

Para os entrevistados, revelou-se igualmente importante garantir a articulação entre os vários departamentos internos da organização, contabilizando 7 unidades de registo. Esta articulação deve ser feita não só com o departamento de IT, para assegurar a recolha de toda a informação técnica do ciberataque, como também com a própria administração e comitê de crise, que tomam as principais decisões de resolução do incidente.

"[...] garantir articulação com as equipas internas e garantir que estas estão a fazer o levantamento certo daquilo que é o enquadramento do ataque, para percebermos exatamente o que é que está em causa [...]" (Cabrita, 2023) (Apêndice 12)

"É de extrema importância a equipa de Comunicação Externa ter um contacto próximo, desde o momento zero, com o centro de tomada de decisão, ou seja, com a administração e comitê de crise, para definição, priorização e sequenciação de mensagens" (Correia, 2023) (Apêndice 9)

A articulação com o departamento de IT é fundamental, sobretudo, para avaliar a extensão do ciberataque, sendo esta outra ação importante levada a cabo pelos entrevistados, com um valor correspondente a 7 unidades de registo. Ao perceberem exatamente a extensão do ataque, os profissionais de Relações Públicas poderão mais facilmente definir um planeamento de comunicação.

"Primeiro, é perceber até que ponto esse ciberataque pode ou não impactar aquilo que é a atividade da organização" (Borges, 2023) (Apêndice 11)

"Obviamente que há aqui um período em que é fundamental, nos ciberataques, nós percebermos qual é que é exatamente a extensão do ataque – foi esta a minha experiência e foi o que eu mais recolhi dessa altura" (Cabrita, 2023) (Apêndice 12)

2.1.2. Implicações para a organização

De forma complementar à subcategoria anterior, é importante explorar as implicações do ciberataque para as organizações entrevistadas para uma melhor compreensão da situação de crise que tiveram de enfrentar.

Tabela 30: Implicações do ciberataque para as organizações

Implicações para a organização	Unidades de registo
Indisponibilidade de serviços	5
Comprometimento de dados pessoais e confidenciais	2
Maior investimento em cibersegurança	**8**

Embora todas as organizações entrevistadas tenham tido implicações diretas do ciberataque, seja na indisponibilidade de serviços ou no comprometimento de dados pessoais e confidenciais, a verdade é que a implicação mais mencionada diz respeito a uma consequência positiva decorrente do próprio incidente, nomeadamente o maior investimento em cibersegurança, com 8 unidades de registo. Segundo os entrevistados, o ciberataque veio alertar não só para a necessidade de um maior investimento em tecnologias de segurança, como também para a importância de formar os colaboradores em cibersegurança.

> *"Eu acho que houve implicações positivas, uma que teve depois como consequência outra. Primeiro, veio alertar para a necessidade de termos sistemas robustos e com segurança. Portanto, fazer investimentos em segurança de IT é um investimento, não é um custo. [...] A segunda evidência que decorre dessa é continuar a investir cada vez mais na segurança da nossa rede. [...] Estou a dizer isto, mas em boa verdade a EDP sempre teve uma boa consciência disto, mas obviamente sempre que há estas situações é um momento de reforço"* (Cabrita, 2023) (Apêndice 12)

> *"As implicações que tem a longo prazo são implicações muitíssimo positivas, na minha opinião. [...] Neste momento, por exemplo, temos em curso um programa de formação em cibersegurança. Uma coisa ligeira no formato, em que são feitos simulacros de phishing com alguma regularidade, para tentar perceber qual é a evolução… Em que vamos dar formação em vídeo, uns mais interativos do que outros. E isto serve à empresa, como é óbvio, mas serve sobretudo aos colaboradores"* (Simões, 2023) (Apêndice 13)

2.2. Importância da comunicação de crise numa situação de ciberataque

Revelou-se necessário compreender a perspetiva dos entrevistados relativamente à importância da comunicação de crise em situação de ciberataque, ou seja, porque motivo devem as organizações apostar na comunicação de crise para uma melhor gestão do incidente.

Tabela 31: Importância da comunicação de crise numa situação de ciberataque

Importância da comunicação de crise	**Unidades de registo**
Partilhar informação	**6**
Garantir a confiança dos *stakeholders*	**7**
Tranquilizar os *stakeholders*	**7**
Permitir que os *stakeholders* tomem medidas perante a situação	2
Proteger a reputação organizacional	4
Garantir o alinhamento de todos os colaboradores	4
Evitar a proliferação de rumores	3
Permitir à organização uma maior capacidade de recuperação do incidente	2

Existe um consenso entre os entrevistados no que respeita ao facto da comunicação de crise ser importante, numa situação de ciberataque, para tranquilizar os *stakeholders*, registando 7 referências. Acima de tudo, a comunicação de crise deve transparecer aos *stakeholders* uma sensação de compromisso da organização com a resolução do problema e, por esse motivo, conferir-lhes uma maior tranquilidade.

> *"Portanto, numa situação como esta, sentir que o stakeholder interno está tranquilo e que, com essa sua tranquilidade, consegue passar também essa segurança para o exterior é fundamental"* (Ramos, 2023) (Apêndice 10)

> *"[...] explicar que estamos a atuar, passar uma mensagem de tranquilidade, passar uma mensagem de que a informação que temos, até ao momento, é parca ainda… Ou seja, uma comunicação que não alimente o pânico, uma comunicação que permita ganhar tempo, mas uma comunicação verdadeira"* (Cabrita, 2023) (Apêndice 12)

Por outro lado, os entrevistados consideram que a comunicação de crise, numa situação de ciberataque, é igualmente importante para garantir a confiança dos *stakeholders*, também com um valor correspondente a 7 unidades de registo. Tal como afirma Loureiro (2023), uma empresa só pode continuar se as pessoas acreditarem nela (Apêndice 8)

"[...] as pessoas têm de saber. Se as pessoas não sabem é logo um problema e começam a perder a confiança em nós" (Simões, 2023) (Apêndice 13)

"[...] a comunicação de crise é algo que nós temos muito presente no nosso dia-a-dia no Instituto, porque as crises que podem afetar a instituição e a confiança que as pessoas têm na instituição são muitas e, portanto, é importante que isso seja assegurado" (Borges, 2023) (Apêndice 11)

"[...] garantir, externamente, as condições de confiança e serenidade junto dos principais stakeholders (clientes, fornecedores, parceiros e cidadãos em geral) [...]" (Correia, 2023) (Apêndice 9)

Destaca-se, ainda, a importância de as organizações apostarem na comunicação de crise, numa situação de ciberataque, por forma a partilhar informação, com um valor correspondente a 6 unidades de registo. Naturalmente, a comunicação é fundamental para as organizações poderem partilhar com os seus *stakeholders* o que está efetivamente a acontecer e informar acerca das implicações que o ciberataque poderá ter não só nos serviços prestados pela organização, como também no comprometimento dos seus dados pessoais.

"[...] a comunicação é fundamental para que todos saibam, de forma transparente e factual, o que está a acontecer" (Loureiro, 2023) (Apêndice 8)

"É fundamental conseguirmos falar com as pessoas, transmitir as informações e assegurar às pessoas que, se precisarem de uma ambulância em caso de acidente ou doença súbita, têm ou não têm acesso a ela" (Borges, 2023) (Apêndice 11)

"[...] procurando assegurar informação fiável sobre os tópicos que podem estar relacionados consigo (como, por exemplo, segurança e proteção de dados, restabelecimento da prestação do serviço em condições de qualidade)" (Correia, 2023) (Apêndice 9)

2.3. Papel do profissional de Relações Públicas numa situação de ciberataque

O profissional de Relações Públicas detém um papel de extrema responsabilidade no processo de resolução de um ciberataque, pelo que se revelou pertinente abordar a perspetiva dos entrevistados relativamente à importância desse papel.

Tabela 32: Papel do profissional de Relações Públicas numa situação de ciberataque

Papel do profissional de Relações Públicas	Unidades de registo
Assumir o controlo de todo o processo de comunicação	**8**
Articular a comunicação com o departamento de IT	**8**
Transformar a informação em mensagens adequadas a cada público	5
Gerir o impacto mediático	2
Manter a calma e tranquilizar todos os envolvidos	**10**
Ter a capacidade de recuperar do incidente e comunicá-lo aos *stakeholders*	1

Segundo a maioria dos entrevistados, o papel do profissional de Relações Públicas, numa situação de ciberataque, passa essencialmente por manter a calma e tranquilizar todos os envolvidos, contabilizando 10 unidades de registo. Como já constatámos anteriormente, a comunicação de crise é fundamental para tranquilizar os *stakeholders* e esse cuidado passa, sobretudo, pela atitude do próprio profissional de Relações Públicas que, perante uma situação marcada pelo desconhecido, incerteza e *stress*, deverá manter a calma e transparecer essa tranquilidade para os próprios *stakeholders* para uma gestão mais eficaz do incidente.

> *"Numa situação de ciberataque, como em qualquer outra situação de crise, o profissional de comunicação é alguém que lá está, que faz parte deste gabinete, e que tem aqui o papel fundamental de manter a calma [...]"* (Ramos, 2023) (Apêndice 10)

> *"[...] a postura, em situação de crise, é sempre uma postura de tranquilidade e de anti-stress"* (Cabrita, 2023) (Apêndice 12)

Os entrevistados afirmaram, ainda, que o profissional de Relações Públicas, numa situação de ciberataque, tem a responsabilidade de assumir o controlo de todo o processo de comunicação, bem como articular a comunicação com o departamento de IT, ambos com 8 unidades de registo.

Por um lado, o profissional de Relações Públicas tem de assumir o controlo de todo o processo de comunicação, por forma a orientar o planeamento da comunicação e garantir que existe um alinhamento de toda a informação que é transmitida.

> *"O trabalho do profissional de Relações Públicas nestas situações de crise é fundamental, porque, no fundo, nós somos aquele elemento de charneira que está ali para comunicar de*

forma eficaz com os diversos públicos aquilo que se está a passar" (Borges, 2023) (Apêndice 11)

"De forma figurada, é um pouco o eixo de transmissão dentro da organização [...]" (Correia, 2023) (Apêndice 9)

"Tem de saber preparar essa circunstância com simulações, com uma visão das operações, saber quem fala, saber quem faz o quê, saber como se articula isso dentro e fora" (Loureiro, 2023) (Apêndice 8)

Sob uma perspetiva diferente, os entrevistados acreditam que o profissional de Relações Públicas tem igualmente de articular a comunicação com o departamento de IT, para garantir a veracidade e fiabilidade de toda a informação que é transmitida, sobretudo tratando-se de uma área tão técnica como a cibersegurança.

"Às vezes eu não sei – e nomeadamente no caso do ciberataque – coisas que são muito técnicas e, portanto, peço que me passem a informação dos tópicos mais relevantes e em que é que isso impacta o quê e quem" (Simões, 2023) (Apêndice 13)

"[...] é informação que vamos buscar e que o chief security officer nos transmite e que nós depois divulgamos [...]" (Borges, 2023) (Apêndice 11)

"Eu, enquanto responsável de comunicação, tenho de fazer a ponte com os especialistas e depois fazer o meu trabalho de bastidores [...]" (Cabrita, 2023) (Apêndice 12)

2.4. Desafios enfrentados pelos profissionais de Relações Públicas numa situação de ciberataque

Da mesma forma que foi importante compreender o papel do profissional de Relações Públicas numa situação de ciberataque, revelou-se pertinente explorar os principais desafios enfrentados na execução do seu papel.

Tabela 33: Desafios enfrentados pelo profissional de Relações Públicas numa situação de ciberataque

Desafios enfrentados pelo profissional de Relações Públicas	Unidades de registo
Tempo limitado	**6**
Cadência de informação nas primeiras horas	1
Instabilidade da informação disseminada	**7**
Capacidade de garantir a veracidade da informação	3

Capacidade de avaliar a informação que pode ser divulgada	**8**
Instabilidade da situação	2
Fugas de informação	1
Conhecimento técnico em cibersegurança	3
Pressão mediática	**10**
Situação inicial marcada pelo desconhecido	1
Público insciente da situação	1
Capacidade de gerir a situação de pagamento de resgate	1
Capacidade de avaliar a extensão do ciberataque	1
Capacidade de justificar a necessidade de comunicação de crise à administração	1
Capacidade de priorizar a saúde mental	2

De entre o conjunto de desafios enfrentados pelo profissional de Relações Públicas numa situação de ciberataque, os entrevistados debruçaram uma maior atenção sobre a pressão mediática, contabilizando 10 unidades de registo. Naturalmente, a ocorrência de um ciberataque, sobretudo de grande amplitude, é motivo de cobertura mediática, pelo que o profissional de Relações Públicas, além de enfrentar as habituais implicações de um ciberataque, poderá lidar com o desafio adicional da pressão mediática.

> *"[...] o responsável do gabinete de crise tem de ter o telefone sempre ligado, porque se acontece às onze da noite e, se não tem resposta, pode vir para fora sem resposta da nossa parte – e não há nada pior do que tentar contactar a empresa e não ser possível obter qualquer declaração… Quando nós temos isto dos media é complicado ou quando temos isto, de facto, a criar impacto na vida das pessoas"* (Ramos, 2023) (Apêndice 10)

> *"Por muita pressão mediática que haja, nós temos de ter a capacidade de aguentar e de perceber que há um trabalho técnico que leva o seu tempo"* (Cabrita, 2023) (Apêndice 12)

> *"Um ciberataque pode provocar uma crise mediática [...] Portanto, acredito que um ciberataque é só mais um fator que um profissional de Relações Públicas tem de estar desperto para que possa acontecer e poder ter de lidar com as suas implicações"* (Borges, 2023) (Apêndice 11)

Outro desafio consideravelmente apontado pelos entrevistados foi a capacidade de avaliar a informação que pode ser divulgada, com um valor correspondente a 8 unidades de registo. É

sabido que as organizações devem reconhecer que foram atacadas e comunicá-lo aos *stakeholders*, mas existe informação que pode comprometer a própria resolução do incidente, pelo que se constitui como um desafio para o profissional de Relações Públicas conseguir avaliar a informação que pode realmente divulgar publicamente.

> *"Durante o ciberataque, é dar aquela informação, como eu já tenho vindo a dizer. Mas apenas a informação que seja útil às pessoas e que ajude a organização a restabelecer-se o mais rápido possível"* (Simões, 2023) (Apêndice 13)

> *"[...] temos de ter muito cuidado com o que vamos dizer, porque o atacante também está a ler notícias. [...] Ou seja, a comunicação tem de ser usada com inteligência, para não estarmos a dar argumentos ou pistas a quem nos ataca daquilo que andamos a fazer. Portanto, muitas vezes o silêncio vale ouro e dar apenas uma mensagem de tranquilidade, que estamos a atuar… Enfim, dando passos pequeninos com informação cirúrgica, sem divulgar dados que possam permitir ao atacante tomar novas posturas [...]"* (Cabrita, 2023) (Apêndice 12)

> *"[...] o facto de eu há pouco estar a referir que tem de haver transparência e clareza na mensagem não quer com isso dizer que devemos dizer tudo a toda a gente e a toda a hora, de todo"* (Ramos, 2023) (Apêndice 10)

A instabilidade da informação disseminada é outro desafio que os entrevistados concordaram que o profissional de Relações Públicas tem de enfrentar, com 7 unidades de registo. Pressionados pelo tempo e pela incerteza característica de uma situação de ciberataque, o profissional de Relações Públicas poderá ter de lidar com a instabilidade da informação que divulga, porque a situação está sempre a evoluir e, a qualquer momento, pode mudar.

> *"Um assessor de imprensa vai sempre procurar responder de forma transparente e mais objetiva possível. No entanto, e com o decorrer do tempo, pode constatar que a informação anteriormente divulgada pode não ter sido totalmente exata. Nesse cenário, é necessário corrigi-la e repor a factualidade, para que a mensagem seja sempre clara"* (Correia, 2023) (Apêndice 9)

> *"[...] o mais chato é nós transmitirmos uma informação que não está completa e depois sermos confrontados, por exemplo, pela comunicação social com algo que nós desconhecemos"* (Borges, 2023) (Apêndice 11)

Importa destacar, ainda, o tempo limitado como um desafio a enfrentar pelo profissional de Relações Públicas numa situação de ciberataque, registando 6 referências. Estando perante um incidente que pode provocar implicações graves à organização, o profissional de Relações Públicas tem de agir o mais rapidamente possível, embora esse facto se possa constituir como um desafio na execução das suas funções.

> *"[...] eu diria que o grande desafio aí é tão rapidamente quanto possível perceber o que é que está, de facto, em causa, o que é que está, de facto, em risco e até que ponto uma área não irá afetar outra"* (Ramos, 2023) (Apêndice 10)

> *"[...] o profissional de comunicação 'joga' com dois fatores principais no caso de um incidente desta natureza: tempo – sendo exigível que responda e aja rápido [...]"* (Correia, 2023) (Apêndice 9)

> *"Foram 6 mil e tal cartas, enviadas o mais rapidamente, porque isto podia ter consequências nas famílias, embora não tenhamos tido conhecimento de nada até agora"* (Simões, 2023) (Apêndice 13)

2.5. Medidas de comunicação em situação de ciberataque

2.5.1. Antes do ciberataque

Revela-se necessário compreender quais as medidas de comunicação que as organizações devem implementar antes do ciberataque, numa ótica de prevenção e mitigação da sua ocorrência.

Tabela 34: Medidas de comunicação – antes do ciberataque

Medidas de comunicação – antes do ciberataque	**Unidades de registo**
Divulgação de boas práticas de cibersegurança junto dos colaboradores	2
Identificação e gestão do risco	1
Definição de um plano de resposta ao incidente	**7**
Realização de simulações	**6**
Mapeamento de *stakeholders*	4
Formação de porta-vozes	3
Execução de um exemplar impresso do manual de crise	1

Segundo os entrevistados, uma das principais medidas de comunicação a implementar pelas organizações antes do ciberataque diz respeito à definição de um plano de resposta ao

incidente, com um valor correspondente a 7 unidades de registo. A verdade é que qualquer organização está sujeita a sofrer um ciberataque, por muito investimento em cibersegurança que tenha, pelo que é importante antecipar a sua ocorrência e, por sua vez, definir todos os procedimentos de resposta ao incidente.

> *"Isso significa ter uma célula de crise identificada, ter dentro da organização a ideia de quais são os primeiros passos caso aconteça uma situação dessas – com quem se fala, quem é que reúne – para poder libertar o CEO para continuar a liderar o negócio num tempo crítico. Acho que tem de haver um esqueleto, chamemos-lhe assim, de uma célula de crise, que é para poder ser ativada no momento em que isso ocorre"* (Loureiro, 2023) (Apêndice 8)

> *"Muito importante, também, é ter o planeamento minimamente feito. Se acontecer um ciberataque, o que é que eu devo fazer?"* (Borges, 2023) (Apêndice 11)

> *"Havendo essa prévia identificação, deve-se perceber, numa situação destas, o que é que eu tenho de fazer, quem é que eu tenho de ativar, o que é que eu devo dizer, o que é que eu posso dizer…"* (Ramos, 2023) (Apêndice 10)

Outra das medidas de comunicação a implementar antes do ciberataque mencionada pelos entrevistados refere-se à realização de simulações, contabilizando 6 unidades de registo. Além de ser importante definir um plano de resposta ao incidente, é também importante testá-lo antes da ocorrência do ciberataque, por forma a garantir a sua operacionalidade.

> *"Deve-se fazer, portanto, alguns simulacros, ou seja, percebermos mesmo, numa situação destas, como é que isto funcionaria. Não basta olhar para o documento e perceber que o número de telefone está lá. A pessoa associada ao contacto está preparada para ser o speaker? Tem as condições necessárias em casa, sobretudo agora com o remoto? Tem rede? Todas estas coisas que nos parecem pequenos detalhes, no momento podem falhar"* (Ramos, 2023) (Apêndice 10)

> *"Preparar significa que as empresas têm de estar preparadas com simulações deste tipo de situações, não só ciber, mas de qualquer tipo de crise"* (Loureiro, 2023) (Apêndice 8)

2.5.2. Durante o ciberataque

Durante o ciberataque, é fundamental o profissional de Relações Públicas tomar um conjunto de medidas de comunicação que permitam a contenção da crise e uma melhor recuperação do incidente.

Tabela 35: Medidas de comunicação – durante o ciberataque

Medidas de comunicação – durante o ciberataque	**Unidades de registo**
Confirmação da ocorrência do ciberataque	2
Divulgação e articulação da gestão do incidente com as autoridades competentes	**10**
Estabelecimento de um plano de ação	5
Recolha do máximo de informação possível sobre o incidente	5
Comunicação, em tempo real, sobre o que está a acontecer	**7**
Utilização de uma comunicação factual, transparente e concisa	**16**
Utilização de uma comunicação cuidada	**9**
Manutenção dos diferentes canais de comunicação atualizados	3
Criação de secções e materiais específicos com informação sobre o ciberataque	1
Realização de uma reunião do gabinete de crise	2
Desenvolvimento de um documento de Q&A sobre o ciberataque	1

Verifica-se um consenso entre os entrevistados no que respeita à utilização de uma comunicação factual, transparente e concisa enquanto medida de comunicação a implementar pelas organizações durante o ciberataque, contabilizando 16 unidades de registo. Tal como sublinha Correia (2023), deve-se comunicar de forma transparentemente responsável, por forma a garantir a recuperação da continuidade do negócio e a reputação da empresa (Apêndice 9)

> *"[...] divulgação de uma comunicação factual, transparente e que permita ao público perceber o que se está a passar"* (Loureiro, 2023) (Apêndice 8)

> *"[...] tem de haver transparência e clareza na mensagem [...]"* (Ramos, 2023) (Apêndice 10)

> *"[...] uma comunicação que não alimente o pânico, uma comunicação que permita ganhar tempo, mas uma comunicação verdadeira. [...] na EDP – e acredito que grande parte dos meus colegas de comunicação – um dos princípios é transparência e verdade da comunicação. Isso deve ser um pilar básico daquilo que é a relação com os media e com todos os nossos stakeholders"* (Cabrita, 2023) (Apêndice 12)

Outra importante medida de comunicação a implementar pelas organizações durante o ciberataque passa pela divulgação e articulação da gestão do incidente com as autoridades competentes, registando um valor correspondente a 10 referências. As organizações devem não só comunicar às autoridades competentes a ocorrência do ciberataque, como também articular com estas a própria gestão do incidente, pelo facto de terem o *know-how* e competências necessárias para saber como reagir eficazmente perante uma situação como esta.

> *"[...] eu diria que temos de ter uma comunicação muito inteligente e, como digo, articulada com as autoridades, porque eles é que são os especialistas nesta matéria. Um ciberataque é um crime muito específico e com alguma sofisticação tecnológica, em alguns casos, de redes internacionais bem montadas, com meios poderosos… Eu acho que é muito importante na comunicação haver uma articulação com as autoridades. Eu diria que é uma das principais regras"* (Cabrita, 2023) (Apêndice 12)

> *"[...] termos a capacidade de envolver todas as pessoas que nos possam aportar algum conhecimento e alguma informação para uma boa resolução [...]"* (Ramos, 2023) (Apêndice 10)

Os entrevistados mencionaram, também, a importância da utilização de uma comunicação cuidada durante o ciberataque, contabilizando 9 unidades de registo. Significa isto que se deve adotar uma comunicação inteligente, partilhando apenas a informação que poderá contribuir para a recuperação do incidente.

> *"Nunca mentir é uma regra, mas dizer tudo, por vezes, também não é a solução"* (Ramos, 2023) (Apêndice 10)

> *"Nós rapidamente percebemos, com uma forte probabilidade, que o ciberataque não era extenso e que o risco de eles terem mais informação era pequeno, portanto optámos por não ser muito extensos na nossa comunicação. O que não significa ausência de comunicação. É gerir a comunicação com inteligência"* (Cabrita, 2023) (Apêndice 12)

De mencionar, ainda, a importância da comunicação, em tempo real, sobre o que está a acontecer durante o ciberataque, com 7 unidades de registo. Sendo um ciberataque uma situação tão imprevisível e mutável, é importante a organização ir atualizando os *stakeholders* acerca da sua evolução.

> *"[...] comunicar absolutamente em tempo real com os seus stakeholders"* (Loureiro, 2023) (Apêndice 8)

"articulação constante entre os vários intervenientes internos para garantir que se fornece toda a informação necessária e útil a cada momento [...]" (Correia, 2023) (Apêndice 9)

"[...] assumir-se um compromisso em que, de hora a hora, se dá um feedback ou explica o ponto de situação" (Ramos, 2023) (Apêndice 10)

2.5.3. Após o ciberataque

Embora tenha sido a fase de crise que os entrevistados conferiram uma menor atenção, é de extrema importância as organizações não esquecerem o pós-crise e, portanto, implementarem medidas de comunicação que lhes permita evitar passar novamente por uma crise semelhante ou mitigar os riscos decorrentes do incidente.

Tabela 36: Medidas de comunicação – após o ciberataque

Medidas de comunicação – após o ciberataque	**Unidades de registo**
Realização de *follow-up* da situação	3
Avaliação dos impactos decorrentes do ciberataque	**5**
Atualização dos planos estratégicos	2

Numa fase de pós-crise, a medida de comunicação mais mencionada pelos entrevistados refere-se à avaliação dos impactos decorrentes do ciberataque, com um valor correspondente a 5 unidades de registo. Durante a gestão do ciberataque, poderão ocorrer falhas e, no sentido de melhor prepararem-se para a eventualidade de um novo ciberataque, as organizações devem avaliar as suas ações e os impactos decorrentes do incidente.

"[...] num pós-crise, é claramente avaliarmos a crise, o que aconteceu, o que poderíamos ter feito de forma diferente, para que da próxima vez que vier a acontecer [...] como é que eu consigo mitigar os riscos da melhor forma, para que tenha o menor impacto e a menor visibilidade" (Ramos, 2023) (Apêndice 10)

"Retiram-se lições aprendidas e tenta-se comunicar de forma que não se voltem a suceder no futuro" (Borges, 2023) (Apêndice 11)

2.6. Importância dos *stakeholders* em situação de ciberataque

Os *stakeholders* assumem um papel fundamental na relação com a organização e, por esse motivo, revelou-se pertinente compreender a perspetiva dos entrevistados relativamente à sua importância no caso específico de um ciberataque.

Tabela 37: Importância dos *stakeholders* em situação de ciberataque

Importância dos *stakeholders*	**Unidades de registo**
Auxiliar a organização na recuperação e mitigação de efeitos decorrentes do incidente	**4**
Tomar as medidas necessárias de proteção e recuperação do ciberataque	2
Assumir o papel de embaixadores da organização, no caso dos colaboradores	**4**

Com um valor igualitário de 4 unidades de registo, os entrevistados concordam que os *stakeholders* são importantes numa situação de ciberataque não só para auxiliar a organização na recuperação e mitigação de efeitos decorrentes do incidente, como também para assumir o papel de embaixadores da organização, no caso dos colaboradores.

Relativamente ao primeiro caso, os entrevistados acreditam que, numa situação de ciberataque, a colaboração e compreensão dos *stakeholders*, sejam eles internos ou externos, poderá ajudar a organização a recuperar mais rapidamente do incidente e a mitigar eventuais danos que possam existir.

> *"Internamente, os colaboradores são indispensáveis, através da sua ação, para recuperar e mitigar os efeitos que o incidente possa provocar – daí que seja necessário que, aqueles que são cruciais para esse restabelecimento, estejam permanentemente na posse da melhor informação possível para desempenhar o seu trabalho; externamente, os clientes, fornecedores e parceiros também têm de estar a par, embora a um ritmo naturalmente menos intenso, da evolução da situação e de como podem ultrapassá-la ou ajudar a ultrapassá-la com a instituição que foi alvo do ataque"* (Correia, 2023) (Apêndice 9)

> *"Posso-lhe dizer também que os únicos stakeholders que tiveram um papel ativo na resolução da crise foram os nossos colaboradores, sem dúvida nenhuma. Houve muitos colaboradores a perder muitas horas de sono – e não me refiro apenas a nível de gestão e direção, estou a falar de operacionais no terreno, nomeadamente na área da logística. Esses foram os heróis. [...] E também creio que, mesmo com a ajuda externa, sem os nossos colaboradores não teríamos resolvido a situação"* (Simões, 2023) (Apêndice 13)

No que se refere ao segundo caso, os entrevistados conferem uma maior atenção aos colaboradores da organização, sublinhando que estes, numa situação de ciberataque, podem assumir o papel de embaixador da organização, ao estarem devidamente informados e ao passar essa mensagem também para o exterior.

"Por vezes, as pessoas podem ter conhecimento de alguma notícia menos boa ou de alguma potencial crise não pelos meios oficiais, digamos assim, e é importante nós também termos canais de comunicação internos bem estabelecidos, para que, em caso de crise ou de uma potencial crise, os nossos trabalhadores, que são a nossa cara junto das pessoas, estejam informados e tenham presente aquilo que se está a passar, para, também eles, poderem assegurar ou não aquilo que se passa e informar as pessoas convenientemente" (Borges, 2023) (Apêndice 11)

"[...] internamente, esclarecer os colaboradores sobre o que está a acontecer, porque eles leem pelas notícias e também sabem e, portanto, um dos princípios básicos é informar primeiro internamente do que externamente. Portanto, os nossos colaboradores, que são embaixadores da nossa marca, também têm amigos, também têm familiares, também leem notícias e, por isso, têm de saber o que se está a passar" (Cabrita, 2023) (Apêndice 12)

2.7. Implicações do ciberataque na reputação organizacional

Constituindo-se como um ativo de grande valor para a organização, a reputação de uma organização poderá ser afetada pela ocorrência de um ciberataque, pelo que se revelou pertinente explorar as implicações que podem ocorrer.

Tabela 38: Implicações do ciberataque na reputação organizacional

Implicações do ciberataque na reputação organizacional	**Unidades de registo**
Imagem negativa da organização	**7**
Perda de confiança dos *stakeholders*	**8**
Perda de clientes	1
Perda de investidores	1
Problemas judiciais	1

Existe um consenso entre todos os entrevistados no que respeita à perda de confiança dos *stakeholders* enquanto implicação do ciberataque na reputação organizacional, com um valor correspondente a 8 unidades de registo. Naturalmente, os *stakeholders* assumem uma relação de compromisso e confiança com a organização e, no caso de comprometimento de dados pessoais ou ausência de explicações, poderão perder a confiança na organização, o que afetará a reputação.

"Tem a ver com a confiança. Ou seja, as implicações são a empresa poder continuar a operar de forma que obtenha a confiança do mercado, dos seus pacientes e dos seus utilizadores ou não" (Loureiro, 2023) (Apêndice 8)

"De uma forma geral, um incidente desta natureza tem consequências negativas na reputação de uma instituição. Pode criar junto dos stakeholders uma sensação de apreensão, dúvida ou desconfiança perante a empresa ou organização com a qual tinha uma relação de previsibilidade e na qual se habituou a confiar. No caso da Vodafone, acredito que a relação próxima e de confiança que há mais de 30 anos mantemos com os nossos clientes foi determinante durante este processo" (Correia, 2023) (Apêndice 9)

"[...] este para mim será sempre o ponto, que é não assumirmos coisas das quais não temos certeza, porque se nós dissermos isto e se vier a confirmar, a confiança fica automaticamente fragilizada. Ou seja, a mim dizem-me 'não houve corrupção de dados, portanto os dados dos clientes estão protegidos' e passado meia hora, uma hora ou uma semana vem-se a comprovar que os dados, de facto, foram acedidos, é natural que haja uma quebra de confiança grande" (Ramos, 2023) (Apêndice 10)

Outra implicação mencionada pela maioria dos entrevistados refere-se à imagem negativa da organização, contabilizando 7 unidades de registo. Sabendo que um ciberataque pode provocar um impacto mediático considerável, é natural que as pessoas passem a percecionar a organização de uma forma diferente após um incidente desta dimensão, sobretudo quando coloca em causa o comprometimento dos seus dados pessoais.

"O risco da desconfiança, o risco da apreensão, o risco da dúvida não esclarecida que, se se prolongarem no tempo, podem deteriorar a imagem pública que clientes e cidadãos têm de determinada organização [...]" (Correia, 2023) (Apêndice 9)

"A nível de imagem corporativa no mercado, isto pode ter impactos nefastos, que não foi o nosso caso" (Simões, 2023) (Apêndice 13)

"Vamos ver, há exemplos que são conhecidos de pessoas que têm as passwords de acesso coladas com post-its no monitor do computador… Portanto, quando isso é do conhecimento público não transmite propriamente uma boa imagem da organização no que diz respeito à cibersegurança. Demonstra até algum desleixo daquilo que deviam ser as funções dos funcionários da organização. Portanto, obviamente que tem impacto para a reputação da organização um ciberataque" (Borges, 2023) (Apêndice 11)

2.8. Implicações do fenómeno de ciberataque na área das Relações Públicas

Por forma a relacionar a área da cibersegurança com a prática das Relações Públicas, mostrou-se pertinente compreender as implicações do fenómeno de ciberataque na área das Relações Públicas.

Tabela 39: Implicações do fenómeno de ciberataque na área das Relações Públicas

Implicações do fenómeno de ciberataque na área das Relações Públicas	**Unidades de registo**
Oportunidade de aprendizagem	**9**
Dificuldade de fortalecimento da atividade	1
Dificuldade de reconstrução de relações com os *Stakeholders*	1
Contexto de rapidez	1
Maior cuidado no estabelecimento da comunicação	1

Contrariando as expectativas previstas inicialmente daquilo que seriam as implicações do fenómeno de ciberataque na área das Relações Públicas, a verdade é que a maioria dos entrevistados concordou que um ciberataque constitui-se como uma oportunidade de aprendizagem para as Relações Públicas, registando um valor de 9 referências. Os entrevistados acreditam que a ocorrência de um ciberataque poderá funcionar como uma oportunidade para a prática da atividade de Relações Públicas, pela exigência comunicacional que se espera numa situação como esta.

> *"Eu acho que é apenas uma oportunidade, porque acho que é preciso comunicar de forma muito profissional, muito verdadeira, muito factual na eventualidade de um ataque cibernético. Por outro lado, um ciberataque não é "se", mas "quando". Portanto, para as empresas é uma oportunidade saberem acompanhar os seus clientes, aconselhá-los nesses momentos que são difíceis tanto para as organizações, como para quem está envolvido como cliente. Acho que é absolutamente uma necessidade e uma oportunidade para a área das Relações Públicas"* (Loureiro, 2023) (Apêndice 8)

> *"Numa crise surgem sempre oportunidades e eu acho que, em contexto de ciberataque, devemos sempre perceber o que podemos aprender com essa situação"* (Ramos, 2023) (Apêndice 10)

De forma conclusiva, importa referir que os resultados obtidos através das entrevistas corroboram, em larga medida, aquilo que os autores já têm vindo a constatar no que toca ao estudo da cibersegurança no contexto da realidade portuguesa, bem como à importância da comunicação de crise em situação de ciberataque, sendo, por isso, um importante contributo para a construção de um guia com propostas de boas práticas sólidas e fundamentadas.

3. Proposta de um Guia de Boas Práticas de Prevenção e Resposta a um Ciberataque

O presente guia de boas práticas constitui-se como o resultado da pesquisa realizada na revisão de literatura, bem como da recolha e interpretação dos dados obtidos através das entrevistas realizadas aos profissionais de Cibersegurança e de Relações Públicas.

Segue-se uma breve introdução relativamente à sua definição e principais objetivos, com o principal intuito de esclarecer a sua relevância para a área da Cibersegurança no contexto das Relações Públicas e para a sua implementação nas organizações portuguesas.

3.1. O conceito de boas práticas

Com origem na literatura durante a era industrial, o conceito de boas práticas materializa-se na ideia de que, embora existam várias abordagens que podem ser utilizadas para alcançar um determinado objetivo, existe normalmente uma única técnica, método ou processo considerado mais eficaz do que os restantes (Michaelson & Stacks, 2014, p. 10). É possível depreender, portanto, que as boas práticas consistem na melhor forma de realizar um determinado processo através do qual as organizações líderes alcançam um melhor desempenho, servindo de exemplo para outras empresas que se esforçam para atingir a excelência (ibidem, 2014, p. 11).

Um guia de boas práticas assume, geralmente, a forma de um conjunto geral de padrões, diretrizes, normas ou parâmetros de referência que orientam a prática, sendo concebidos para melhor o desempenho (Seeger, 2006, p. 233). Não obstante, o que funciona num setor pode ter uma aplicabilidade muito limitada noutro, o que significa que a adaptação generalizada de boas práticas deve ser feita de forma prudente e com conhecimento profundo dos fatores contextuais e das variáveis situacionais (ibidem, 2006, p. 233). As boas práticas também podem ser percecionadas como lições mais amplas para a aprendizagem organizacional e profissional num determinado local de prática (ibidem, 2006, p. 233).

Posto isto, importa ressalvar que as práticas recomendadas no presente guia têm por base a perspetiva de profissionais representantes de diferentes organizações, inseridas em diferentes

setores, estando, portanto, condicionadas à experiência pessoal do seu setor. Ainda assim, procurou-se abranger um leque diversificado de entrevistados, além da própria revisão da literatura, precisamente para se conseguir elaborar um guia que, de forma geral, ofereça orientações genéricas e sirva de inspiração a todos os profissionais.

3.2. A quem se destina o guia

O presente guia de boas práticas destina-se a todos os estudantes, profissionais ou interessados no tema da prevenção e resposta a um ciberataque.

3.3. Objetivo do guia

O principal objetivo deste guia passa pela partilha de boas práticas de prevenção e resposta a um ciberataque, a serem eventualmente implementadas pelos profissionais de Relações Públicas nas organizações, no sentido de garantir uma melhor recuperação do incidente e a manutenção da reputação organizacional.

3.4. Valor do guia

Sendo a Cibersegurança uma preocupação atual nas organizações, sobretudo pelo aumento significativo do número de ciberataques, e verificando-se uma lacuna na literatura portuguesa no que respeita ao estudo da comunicação de crise em contexto de ciberataque, o presente guia constitui-se como uma mais valia não só a nível académico, como também a nível organizacional. Por um lado, possibilita a criação de conhecimento sobre prevenção e resposta a um ciberataque, adaptado ao contexto português e, portanto, desenvolvido especificamente para as organizações portuguesas. Adicionalmente, reúne-se num único documento todo o processo de gestão de um ciberataque, desde a mitigação até à sua resolução, através da divulgação de boas práticas de prevenção, bem como orientações de resposta ao incidente, que poderão servir de inspiração a organizações que estejam perante uma situação de ciberataque ou que pretendam prevenir a sua ocorrência.

Numa vertente de carácter mais teórico, o guia é desenvolvido tendo por base evidências teóricas de investigadores e estudiosos da área, mas igualmente complementado pela experiência e conhecimento de profissionais especializados no tema, inclusive organizações que foram recentemente alvo de um ciberataque. Além disso, apresentam-se prospetivas e tendências futuras que poderão ajudar as organizações a melhor prepararem-se em função desse contexto de mudança.

3.5. Como está organizado o guia

O guia inicia-se com uma breve introdução, em que é explícito o seu propósito e metodologia de construção, seguindo-se uma designação dos principais conceitos abordados no estudo.

No sentido de melhor esclarecer o leitor, segue-se uma explicação acerca da importância de as organizações definirem uma estratégia de prevenção e resposta ao ciberataque, esclarecendo de que forma esta estratégia poderá impactar a resolução da crise e minimizar os danos decorrentes do incidente. Além disso, revela-se pertinente elucidar o leitor acerca do atual panorama de ciberataques em Portugal e das principais tendências e desafios na área da cibersegurança, para, no caso particular das organizações, se poderem preparar convenientemente em função do contexto em que atuam.

Segue a apresentação das boas práticas, organizadas consoante a sua área e propósito, tal como se procedeu na análise das entrevistas: por um lado, recomendações ao nível da cibersegurança, numa ótica de prevenção do ciberataque; por outro lado, recomendações em termos de comunicação, apresentadas tendo por base as diferentes fases da gestão de crise: pré-crise, crise e pós-crise.

Por último, surgem as notas finais, que apresentam uma breve conclusão acompanhada de algumas considerações acerca do presente guia de boas práticas.

O Guia de Boas Práticas de Prevenção e Resposta a um Ciberataque pode ser consultado, em detalhe, no Apêndice 16.

Conclusões

Embora existam já alguns estudos que comprovam a importância da atividade de Relações Públicas na gestão de um ciberataque, a presente dissertação surge no sentido de colmatar uma falha existente na literatura portuguesa no que respeita à interligação destas duas áreas tão distintas, sobretudo numa ótica de prevenção e resposta ao ciberataque.

O crescente aumento das ciberameaças, nos últimos anos, tem provocado inúmeros desafios às organizações, sobretudo no que se refere à proteção dos seus sistemas de informação e à capacidade de recuperar de um ciberataque. As organizações estão cada vez mais expostas, em resultado do avanço tecnológico e da sofisticação das técnicas e ferramentas utilizadas nos ciberataques, provocando uma sensação de ameaça e incerteza cada vez maior.

Perante este cenário, revelou-se pertinente reunir, por um lado, a perspetiva de diferentes especialistas e profissionais da área da Cibersegurança relativamente ao atual panorama de ciberataques em Portugal, bem como à importância de as organizações estarem devidamente seguras e preparadas para a eventualidade de um ciberataque. Sendo a Cibersegurança uma área tão particular e complexa, procurou-se compreender igualmente o ponto de vista dos entrevistados em relação às principais tendências e desafios inerentes à área, que poderão, de alguma forma, comprometer ou exigir uma adaptação de aquilo que é a aplicação da Cibersegurança até ao momento.

Em complementaridade, revelou-se necessário compreender a perspetiva de diferentes especialistas e profissionais da área das Relações Públicas em relação à importância da comunicação de crise no processo de gestão de um ciberataque. Sendo a comunicação de crise uma necessidade absoluta para garantir uma rápida e melhor recuperação do incidente e assegurar a manutenção da reputação organizacional, revelou-se igualmente pertinente abordar o papel fundamental do profissional de Relações Públicas neste processo que, muitas vezes, enfrenta um conjunto de desafios que dificultam a execução da sua função.

Em função da pergunta de partida estabelecida para orientar o presente estudo – *"Como é que os profissionais de Relações Públicas podem contribuir para a preparação das organizações em situação de ciberataque, no contexto português?"* –, é possível concluir que, numa primeira instância, é fundamental os profissionais de Relações Públicas estarem a par do atual panorama de ciberataques em Portugal e estar cientes dos problemas que a sua organização poderá vir a enfrentar se for alvo de um ciberataque para, numa fase posterior, terem não só a capacidade de antecipar eventuais danos, numa ótica de prevenção e em constante articulação com o

departamento de IT, como também conseguirem preparar a organização da melhor forma possível para a eventualidade de um ciberataque, sobretudo no que toca à gestão do incidente. A proposta de guia de boas práticas apresentada como resultado final deste estudo constitui-se, portanto, como uma solução prática e orientadora da forma como os profissionais de Relações Públicas devem atuar no sentido de melhor prepararem as suas organizações em situação de ciberataque.

Por forma a melhor esclarecer os resultados obtidos no decorrer do estudo, revela-se pertinente explorar, individualmente, as conclusões de cada objetivo específico.

Objetivo 1: Desenvolver um quadro teórico sobre Cibersegurança no contexto das Relações Públicas em Portugal.

O primeiro objetivo de investigação estabeleceu-se com o intuito de aprofundar o estado da arte de Cibersegurança aplicado às necessidades de conhecimento dos profissionais de Relações Públicas no sentido de atuarem perante uma situação de ciberataque. Sendo a Cibersegurança uma área tão particular e complexa e, por esse motivo, nem sempre compreendida pelas restantes áreas, revela-se fundamental que, no caso particular de resposta a um ciberataque, o profissional de Relações Públicas tenha noções básicas não só sobre a área da Cibersegurança em si, mas também sobre o atual panorama de ciberataques a nível nacional para, em função desse conhecimento e do contexto em que atua, melhor desenvolver a sua função. Neste sentido, as entrevistas realizadas aos especialistas e profissionais de Cibersegurança revelaram-se fundamentais para aprofundar este conhecimento aplicado à realidade portuguesa.

Numa primeira instância, a aplicação das entrevistas permitiu aferir que existe uma maior preocupação relativamente à atual fase de Guerra Cibernética, em que o número de ciberataques tem aumentado significativamente, confirmando as estatísticas partilhadas pelos relatórios consultados (Centro Nacional de Cibersegurança, 2023; Check Point, 2023b; S21sec, 2023). À semelhança da perspetiva de Alexandrou (2021), também os entrevistados consideram que os atuais ciberataques se caracterizam por uma maior complexidade, sofisticação das técnicas utilizadas e emergência do cibercrime enquanto atividade económica, sobretudo no que se refere aos conflitos entre diferentes nações.

No caso específico do contexto português, tal como evidenciado no *Relatório Riscos & Conflitos* (Centro Nacional de Cibersegurança, 2023), os entrevistados referem 2022 como o ano que marcou uma maior ocorrência de ciberataques de grande magnitude, em consequência de dois grandes fatores: pandemia de Covid-19 e transformação digital, confirmando a ideia defendida por Aslan *et al.* (2023). Os entrevistados confirmam, igualmente, as tendências partilhadas pelo Centro

Nacional de Cibersegurança (2023) no que se refere ao atual panorama de ciberataques em Portugal, caracterizado pela maior frequência do *ransomware* e do *phishing*, sobretudo em setores como a saúde, a educação, a administração pública e a banca, provocando às organizações riscos como a paralisação temporária de atividade, o comprometimento de dados pessoais e confidenciais, quebra financeira e o pagamento de resgate, em caso de *ransomware*.

Perante este cenário, os entrevistados defendem a absoluta necessidade de as organizações apostarem em políticas de cibersegurança, no sentido de prevenir a ocorrência de ciberataques, garantir uma maior capacidade de recuperação de um incidente e evitar disrupção de serviço, da mesma forma que Chen (2023) enaltece a importância da cibersegurança para uma gestão eficaz do incidente. Sendo cada vez mais importante as organizações promoverem uma cultura centrada na cibersegurança (Fisher *et al.*, 2021), os entrevistados referem um aumento generalizado do grau de maturidade das empresas portuguesas em cibersegurança, confirmando as prospetivas do relatório *Top 7 Trends Shaping Digital Transformation in 2023* (MuleSoft, 2022) de que 2023 seria caracterizado por um aumento do investimento em cibersegurança por parte das empresas, embora sublinhem o facto de as PME's ainda não estarem suficientemente preparadas, representando um dos principais desafios da implementação da cibersegurança nas organizações mencionados por Hussain *et al.* (2020). A constituição de uma cultura de cibersegurança sólida pode ser alcançada através da consciencialização, formação e educação dos colaboradores em matéria de cibersegurança (Gonçalves, 2019), perspetiva igualmente defendida pelos entrevistados, que acrescentam medidas essenciais como a gestão de identidades e acessos, através da definição de políticas de *password* fortes e ativação do múltiplo fator de autenticação, e o investimento em tecnologia, validando as medidas partilhadas pelo Centro Nacional de Cibersegurança (2023), pela Check Point (2023) e pela ENISA (2021).

À semelhança das ameaças referidas pelo Centro Nacional de Cibersegurança (2023), pela Deloitte (2023), por Drolet (2023) ou por Hussain *et al.* (2020), os entrevistados acreditam que a cibersegurança tem vindo a ser influenciada por grandes tendências tecnológicas, como sendo a Inteligência Artificial, o 5G e a *Internet of Things*, acrescentando a computação quântica à ideia partilhada pelos referidos autores. Aliado a estas tendências, os entrevistados referem um conjunto de desafios inerentes à atuação da cibersegurança, como sendo o fator humano, a complexidade dos ciberataques, a falta de cultura de cibersegurança nas organizações portuguesas e as tecnologias emergentes, tal como referem o Centro Nacional de Cibersegurança (2023) e Hussain *et al.* (2020). Acredita-se que o futuro dos ciberataques, no contexto português, passará, essencialmente, por uma maior influência das tecnologias emergentes que, naturalmente,

provocará um aumento significativo do número de ciberataques, cada vez mais sofisticados, tal como prevê o Centro Nacional de Cibersegurança (2023).

Para uma eficaz gestão de um ciberataque, os entrevistados acreditam que a comunicação assume um papel fundamental, possibilitando à organização uma melhor recuperação do incidente e manutenção da reputação, perspetiva igualmente defendida por Wang e Park (2017), sendo a Vodafone apontada como o melhor exemplo nesta questão, o que confirma a opinião de Lino Santos, coordenador do CNCS, relativamente à transparência da comunicação e gestão de crise exemplares da Vodafone (Santos in Caçador, 2022b). Neste sentido, os entrevistados acreditam que a comunicação é importante para informar e esclarecer os *stakeholders* acerca do incidente, sendo fundamental as organizações utilizarem uma comunicação factual e transparente, ainda que utilizada de forma cuidada, tal como referem Manley e Mclntire (2021).

Objetivo 2: Compreender a perspetiva de profissionais de Relações Públicas sobre o papel que desempenham numa situação de ciberataque.

Face a uma lacuna existente na literatura portuguesa acerca da importância da comunicação de crise no processo de gestão de um ciberataque, verificou-se a necessidade de aprofundar o tema e compreender de que forma os profissionais de Relações Públicas podem contribuir para a mitigação do risco, minimização dos danos e recuperação do ciberataque. Para o efeito, procedeu-se à realização de entrevistas a especialistas e profissionais de Relações Públicas que, através das suas experiências e conhecimentos, permitiram responder ao presente objetivo de investigação.

A realização das entrevistas permitiu concluir que, no caso das quatro organizações em estudo que foram alvo de um ciberataque, o seu modo de atuação passou, sobretudo, por informar os *stakeholders* sobre o incidente, avaliar a extensão do ciberataque e garantir a articulação entre os vários departamentos internos da organização, resultando o ciberataque numa implicação positiva para a organização, nomeadamente o maior investimento em cibersegurança.

Sob uma perspetiva mais geral, os entrevistados defendem que a comunicação de crise é fundamental numa situação de ciberataque, confirmando a perspetiva de Mpholo (2022) de que a maioria das organizações considera estratégico envolver a função de Relações Públicas na sua abordagem de gestão do incidente. Estando ciente de que, numa situação de ciberataque, a comunicação desempenha um papel particularmente significativo na partilha de informação, na construção de relações e na promoção da confiança (Manley & Mclntire, 2021), também os entrevistados acreditam que a comunicação é fundamental, sobretudo, no sentido de tranquilizar os *stakeholders*, procurando garantir a sua confiança, e partilhar informação sobre o incidente.

Assumindo o papel fundamental de ponte de comunicação entre uma organização, os seus *stakeholders* e os órgãos de comunicação social (Kim *et al.*, 2017), os entrevistados referem que o profissional de Relações Públicas deve, acima de tudo, manter a calma e tranquilizar todos os envolvidos, assumir o controlo de todo o processo de comunicação e manter a articulação permanente com o departamento de IT. Não obstante, este profissional enfrenta um conjunto de desafios na execução do seu papel, entre os quais os entrevistados destacam: a pressão mediática, sendo que Manley e Mclntire (2021) enaltecem a necessidade de gestão dos órgãos de comunicação social enquanto componente chave do planeamento de comunicação, precisamente para contrariar especulações e rumores; a capacidade de avaliar a informação que pode ser divulgada, desafio igualmente mencionado pelo Ministério do Interior da República da Sérvia (2019); a instabilidade da informação disseminada; e, ainda, o tempo limitado, que Wang e Park (2017) consideram o fator mais importante para moldar a perceção pública sobre a responsabilidade da organização no tratamento do incidente e, subsequentemente, sobre a sua reputação.

Numa ótica de prevenção do ciberataque, em que a comunicação de crise se centra na localização e redução do risco, por forma a prevenir a ocorrência de uma eventual crise (Coombs & Holladay, 2010), os entrevistados defendem que as organizações devem, essencialmente, definir um plano de resposta ao incidente, tal como afirmam o Centro Nacional de Cibersegurança (2024), Manley e Mclntire (2021) e Santos (2021), o qual beneficiará a capacidade da organização para lidar com este tipo de incidentes, uma vez que as equipas funcionarão de forma mais eficiente (Manley & Mclntire, 2021). Além disso, os entrevistados destacaram a necessidade das organizações realizarem simulações de um eventual ciberataque, para melhor se prepararem para a sua eventualidade, perspetiva igualmente partilhada pelo Centro Nacional de Cibersegurança (2024), que recomenda a testagem do plano de comunicação através de exercícios de simulação.

Durante o incidente, em que a comunicação gera um efeito significativo sobre os resultados da crise, como sendo o número de vítimas e a quantidade de danos reputacionais sofridos pela organização (Coombs & Holladay, 2010), os entrevistados acreditam que as organizações devem, sobretudo: adotar uma comunicação factual, transparente e concisa, ainda que de forma cuidada, à semelhança da perspetiva defendida por Manley e Mclntire (2021); divulgar e articular a gestão do incidente com as autoridades competentes, tal como recomenda o Centro Nacional de Cibersegurança (2024); e comunicar, em tempo real, o que está a acontecer, assegurando uma comunicação frequente com os *stakeholders* ao longo do ciclo de vida do incidente, tal como sublinham Manley e Mclntire (2021). Este processo de comunicação deve basear-se na premissa da teoria situacional de comunicação de crise, que argumenta que cada resposta a uma crise deve

começar com a informação de instrução e informação de ajustamento e, em função do tipo de crise, tentar esforços de reparação da reputação através das restantes estratégias de resposta (Coombs & Holladay, 2010).

Após o ciberataque, em que a comunicação se constitui, em grande parte, como uma extensão da comunicação de resposta à crise, juntamente com a aprendizagem da crise por parte da organização (Coombs & Holladay, 2010), os entrevistados referem ser fundamental avaliar os impactos decorrentes do incidente, por forma a atualizar os planos estratégicos com as lições aprendidas na gestão da situação, ideia igualmente partilhada pelo Centro Nacional de Cibersegurança (2024) e por Santos (2021).

No que se refere aos *stakeholders*, estes assumem um papel fundamental numa situação de ciberataque, na medida em que não só auxiliam a organização na recuperação e mitigação de efeitos decorrentes do incidente, como também, no caso dos colaboradores, assumem o papel de embaixadores da organização. Tal como afirma Sapriel (2021), o envolvimento rápido, ativo e regular dos *stakeholders*, numa situação de ciberataque, revela-se crítico para manter a confiança, sobreviver à crise e possivelmente emergir mais forte, sendo, por esse motivo, o mapeamento dos *stakeholders* o ponto de partida para comunicar de forma sensível e eficaz e, assim, evitar prejudicar a reputação organizacional.

Segundo os entrevistados, um ciberataque pode ter grandes implicações na reputação organizacional, tal como referem Wang e Park (2017). Tendo por base a perspetiva de Kim e Lee (2018) de que as pessoas têm vindo a desconfiar cada vez mais da competência das organizações, a verdade é que os entrevistados acreditam que as implicações na reputação se podem traduzir precisamente na perda de confiança dos *stakeholders*, bem como na imagem negativa que poderá estar associada à organização, ou seja, a impressão que as pessoas poderão vir a ter da organização (Barnett *et al.*, 2006). Este facto corrobora a teoria situacional de comunicação de crise, que assume que a reputação de uma organização é um recurso valioso ameaçado por crises e, por esse motivo, acredita-se que uma resposta comunicativa estratégica pode ajudar a proteger o recurso de reputação ao selecionar uma estratégia de resposta à crise que se ajuste à situação de crise (Coombs & Holladay, 2002).

Embora um ciberataque se possa transformar numa eventual situação de crise, os entrevistados acreditam que a sua ocorrência poderá ser uma oportunidade de aprendizagem para a área das Relações Públicas, confirmando as teorias de Bundy *et al.* (2016), Coombs e Holladay (2010) e Pearson e Mitroff (1993) de que qualquer crise resulta numa aprendizagem organizacional.

Objetivo 3: Elaborar uma proposta de guia de boas práticas de prevenção e resposta a um ciberataque a implementar pelos profissionais de Relações Públicas nas organizações.

Apresentando-se como o resultado final que conjuga a perspetiva dos especialistas entrevistados e as evidências teóricas exploradas na revisão da literatura, a proposta de guia de boas práticas de prevenção e resposta a um ciberataque constituiu-se como uma solução prática e pertinente às organizações portuguesas, na tentativa de colmatar a lacuna existente na literatura portuguesa. Além da apresentação das conclusões acerca do tema em questão, revelou-se essencial a construção de um documento com um conjunto de boas práticas que permitisse oferecer orientações genéricas e servir de inspiração a todos os interessados na prevenção e resposta a um ciberataque.

Por esse motivo, acredita-se que a presente dissertação, além de se constituir como um contributo fundamental para a literatura académica pela sua inovação, relevância e atualidade, poderá fornecer, em termos práticos, um exemplo de boas práticas a seguir pelas organizações no processo de gestão de crise motivada por um ataque informático.

Embora o estudo forneça importantes resultados no que respeita à prevenção e resposta a um ciberataque, em particular no contexto português, existem limitações que devem ser mencionadas, nomeadamente no que respeita à realização das entrevistas. Como é possível constatar no capítulo referente à metodologia, foram contactados 33 profissionais ou especialistas em Cibersegurança e Relações Públicas e a amostra do presente estudo é constituída somente por 12 entrevistados. Assim sendo, a grande limitação prendeu-se com a impossibilidade de realizar algumas entrevistas que seriam um contributo fundamental para o desenvolvimento do estudo, pelo facto de contribuírem para a discussão em torno do tema e permitirem um confronto entre um maior número de perspetivas. Além disso, a limitação de tempo aliada ao facto de o estudo se restringir apenas ao contexto português, não existindo uma comparação com outros países, poderá constituir-se como uma limitação evidenciada na presente investigação.

Para investigações futuras, seria interessante estudar em profundidade casos específicos de ciberataque em organizações portuguesas considerados exemplos de sucesso no que toca à gestão do incidente, sobretudo em setores como a saúde e a educação, por forma a compreender a estratégia e o modo de atuação que permitiram recuperar do incidente e assegurar a reputação organizacional. Além disso, seria importante perceber até que ponto os profissionais de Relações Públicas em Portugal estão efetivamente preparados para a gestão de um ciberataque quando comparados com profissionais internacionais e, dessa forma, retirar lições das melhores práticas implementadas ao nível da prevenção e resposta a um ciberataque por organizações mundiais.

Referências Bibliográficas

2023 Cyber Security Report. (2023a). Check Point. https://go.checkpoint.com/2023-cyber-security-report/

2023 Global Future of Cyber Survey. (2022). Deloitte. https://www.deloitte.com/content/dam/assets-shared/legacy/docs/analysis/2022/deloitte_future_of_cyber_2023.pdf

2023 Mid-Year Cyber Security Report. (2023b). Check Point. https://pages.checkpoint.com/2023-mid-year-cyber-security-report.html

Agrafiotis, I., Nurse, J., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), 1-15. https://doi.org/10.1093/cybsec/tyy006

Alexandrou, A. (2021). *Cybercrime and Information Technology: Theory and Practice - The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices*. Taylor & Francis Group.

Andrade, F. P., Fonseca, I., Silva, J. A., Abreu, J. C., Jerónimo, P., Venâncio, P. D., & Freitas, P. M. (2020). *Relatório Cibersegurança em Portugal: Ética & Direito*. Observatório de Cibersegurança. https://www.cncs.gov.pt/docs/relatorio-eticadireito2020-observatoriociberseguranca-cncs.pdf

Aslan, Ö., Aktug, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, *12*(6), 1-42. https://doi.org/10.3390/electronics12061333

Asllani, A., White, C. S., & Ettkin, L. (2013). Viewing Cybersecurity as a Public Good: The Role of Governments, Businesses, and Individuals. *Journal of Legal, Ethical and Regulatory Issues*, *16*(1), 7-14.

Associação para a Promoção e Desenvolvimento da Sociedade de Informação. (2023, março). *Glossário da Sociedade de Informação*. https://apdsi.pt/glossario/

Barnett, M. L., & Hoffman, A. (2008). Beyond Corporate Reputation: Managing Reputational Interdependence. *Corporate Reputation Review*, *11*(1), 1-9. 10.1057/crr.2008.2

Barnett, M. L., Jermier, J. M., & Lafferty, B. A. (2006). Corporate Reputation: The Definitional Landscape. *Corporate Reputation Review*, *9*(1), 26-38. https://doi.org/10.1057/palgrave.crr.1550012

Barros, G. O. (2018). *A Cibersegurança em Portugal*. Gabinete de Estratégia e Estudos: Ministério da Economia.

Bentley, J. M., Oostman, K. R., & Shah, S. F. (2017). We're sorry but it's not our fault: Organizational apologies in ambiguous crisis situations. *Journal of Contingencies and Crisis Management*, *26*(1), 1-12. https://doi.org/10.1111/1468-5973.12169

Berens, G., & van Riel, C. (2004). Corporate Associations in the Academic Literature: Three Main Streams of Thought in the Reputation Measurement Literature. *Corporate Reputation Review*, *7*(2), 161-178. 10.1057/palgrave.crr.1540218

Bernays, E. L (2015). *Crystallizing Public Opinion*. Open Road Integrated Media. (Obra original publicada em 1923)

Blaikie, N. (2010). *Designing Social Research: The Logic of Anticipation*. Polity Press.

Botan, C. H., & Taylor, M. (2004). Public Relations: State of the Field. *Journal of Communication*, *54*(4), 645-661. https://doi.org/10.1111/j.1460-2466.2004.tb02649.x

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, *9*(2), 27-40. https://doi.org/10.3316/QRJ0902027

Broom, G. M., & Sha, B. (2013). *Cutlip and Center's Effective Public Relations*. Pearson Education.

Bryman, A. (2012). *Social research methods*. Oxford University Press.

Bundy, J., Pfarrer, M. D., Short, C. E., & Coombs, W. T. (2016). Crises and Crisis Management: Integration, Interpretation, and Research Development. *Journal of Management*, *43*(6), 1-32. https://doi.org/10.1177/0149206316680030

Burnett, J. J. (1998). A Strategic Approach To Managing Crises. *Public Relations Review*, *24*(4), 475-488. https://doi.org/10.1016/S0363-8111(99)80112-X

Butterick, K. (2011). *Introducing Public Relations: Theory and Practice*. SAGE Publications.

Caçador, F. (2022a, outubro 28). 2022 foi um “ano terrível” para a cibersegurança em Portugal e especialistas avisam que 2023 pode ser pior. *Sapo Tek.* https://tek.sapo.pt/noticias/computadores/artigos/2022-foi-um-ano-terrivel-para-a-ciberseguranca-em-portugal-e-especialistas-avisam-que-2023-pode-ser-pior

Caçador, F. (2022b, fevereiro 09). Ataque à Vodafone: Transparência na comunicação e gestão de crise elogiadas como boas práticas. Sapo Tek. https://tek.sapo.pt/noticias/computadores/artigos/ataque-a-vodafonetransparencia-na-comunicacao-e-gestao-de-crise-elogiadas-como-boas-praticas

Câmara Municipal de Loures alvo de ciberataque "malicioso e deliberado". (2022a, setembro 22). *Diário de Notícias*. https://www.dn.pt/local/camara-municipal-de-loures-alvo-de-ciberataque-malicioso-e-deliberado-15189231.html

Carballo-Cruz, F. (Coord.) (2022). Relatório Cibersegurança em Portugal. Observatório de Cibersegurança. https://www.cncs.gov.pt/docs/relatorio-economia2022-obciber-cncs.pdf

Cavelty, M. D., & Egloff, F. J. (2019). The Politics of Cybersecurity: Balancing Different Roles of the State. *St Antony’s International Review*, *15*(1), 37-57. https://ssrn.com/abstract=3403971

Centro Nacional de Cibersegurança (2023). *Relatório Riscos & Conflitos*. Observatório de Cibersegurança. https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf

Centro Nacional de Cibersegurança (2024). *Referencial de Comunicação de Risco e de Crise em Cibersegurança*. Observatório de Cibersegurança. https://www.cncs.gov.pt/docs/ref-com-crisecncs.pdf

Chen, E. T. (2023). The Importance of Cybersecurity for Organizations: Implementing Cybersecurity to Prevent Cyberattacks. In Verma, S., Vyas, V., & Kaushik, K. (coords.). *Cybersecurity Issues, Challenges, and Solutions in the Business World* (pp. 46-58). IGI Global.

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*, 1-8. https://doi.org/10.1016/j.chbr.2022.100167

Chun, R. (2005). Corporate reputation: Meaning and measurement. *International Journal of Management Reviews*, *7*(2), 91-109. https://doi.org/10.1111/j.1468-2370.2005.00109.x

Ciberataque expôs nomes de 14 mil trabalhadores da Segurança Social. (2023, janeiro 11). *Jornal de Notícias*. https://www.jn.pt/justica/ciberataque-expos-nomes-de-14-mil-trabalhadores-da-seguranca-social-15638745.html

Cipriano, R. (2022, janeiro 19). Ataque informático ao Comité Internacional da Cruz Vermelha compromete dados sobre mais 500 mil "pessoas altamente vulneráveis". *Observador*. https://observador.pt/2022/01/19/ataque-informatico-ao-comite-internacional-da-cruz-vermelha-compromete-dados-sobre-mais-500-mil-pessoas-altamente-vulneraveis/

Claeys, A., Cauberghe, V., & Vyncke, P. (2010). Restoring reputations in times of crisis: An experimental study of the Situational Crisis Communication Theory and the moderating effects of locus of control. *Public Relations Review*, *36*(3), 256-262. https://doi.org/10.1016/j.pubrev.2010.05.004

Comer, D. E. (2015). *Computer Networks and Internets*. Pearson Education Limited.

Coombs, W. T. (1995). Choosing the Right Words: The Development of Guidelines for the Selection of the "Appropriate" Crisis-Response Strategies. *Management Communication Quarterly*, *8*(4), 447-476. https://doi.org/10.1177/0893318995008004003

Coombs, W. T. (1998). An Analytic Framework for Crisis Situations: Better Responses From a Better Understanding of the Situation. *Journal of Public Relations Research*, *10*(3), 177-191. https://doi.org/10.1207/s1532754xjprr1003_02

Coombs, W. T. (2004). Impact of Past Crises on Current Crisis Communication: Insights From Situational Crisis Communication Theory. *International Journal of Business Communication*, *41*(3), 265-289. https://doi.org/10.1177/0021943604265607

Coombs, W. T. (2006). The Protective Powers of Crisis Response Strategies: Managing Reputational Assets During a Crisis. *Journal of Promotion Management*, *12*(3-4), 241-260. https://doi.org/10.1300/J057v12n03_13

Coombs, W. T. (2007). Protecting Organization Reputations During a Crisis: The Development and Application of Situational Crisis Communication Theory. *Corporate Reputation Review*, *10*(3), 163-176. 10.1057/palgrave.crr.1550049

Coombs, W. T. (2019). *Ongoing Crisis Communication: Planning, Managing, and Responding*. SAGE Publications. (Obra originalmente publicada em 1999)

Coombs, W. T. (2014). The value of communication during a crisis: Insights from strategic communication research. *Business Horizons*, *58*(2), 141-148. https://doi.org/10.1016/j.bushor.2014.10.003

Coombs, W. T., & Holladay, S. J. (1996). Communication and Attributions in a Crisis: An Experimental Study in Crisis Communication. *Journal of Public Relations Research*, *8*(4), 279-295. https://doi.org/10.1207/s1532754xjprr0804_04

Coombs, W. T., & Holladay, S. J. (2001). An Extended Examination of the Crisis Situations: A Fusion of the Relational Management and Symbolic Approaches. *Journal of Public Relations Research*, *13*(4), 321-340. https://doi.org/10.1207/S1532754XJPRR1304_03

Coombs, W. T., & Holladay, S. J. (2002). Helping Crisis Managers Protect Reputational Assets: Initial Tests of the Situational Crisis Communication Theory. *Management Communication Quarterly*, *16*(2), 165-186. https://doi.org/10.1177/089331802237233

Coombs, W. T., & Holladay, S., J. (2006). Unpacking the halo effect: reputation and crisis management. *Journal of Communication Management*, *10*(2), 123-137. https://doi.org/10.1108/13632540610664698

Coombs, W. T., & Holladay, S. J. (2010). *The Handbook of Crisis Communication*. Wiley-Blackwell.

Costa, R. O. (2022, novembro 21). Câmara Municipal de Faro alvo de ataque informático. *TSF*. https://www.tsf.pt/portugal/sociedade/camara-municipal-de-faro-alvo-de-ataque-informatico-15374132.html

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13-21. 10.22215/timreview835

Creswell, J. W. (2003). *Research Design: Qualitative, quantitative, and mixed method approaches*. SAGE publications.

Cyber Security Culture in organisations. (2017). ENISA. https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

Cybersecurity: A Generic Reference Curriculum. (2016). NATO. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/20161025_1610-cybersecurity-curriculum.pdf

Cybersecurity guide for SMEs - 12 steps to securing your business. (2021). ENISA. https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes

Davies, G., & Miles, L. (1998). Reputation Management: Theory versus Practice. *Corporate Reputation Review*, *2*(1), 16-27. 10.1057/PALGRAVE.CRR.1540064

Davies, G., Chun, R., & da Silva, R. (2001). The Personification Metaphor as a Measurement Approach for Corporate Reputation. *Corporate Reputation Review*, *4*(2), 113–127. https://doi.org/10.1057/palgrave.crr.1540137

Davies, G., Chun, R., da Silva, R., & Roper, S. (2003). *Corporate Reputation and Competitiveness*. Routledge.

Daymon, C., & Holloway, I. (2005). *Qualitative Research Methods in Public Relations and Marketing Communications*. Routledge.

Decreto-Lei n.º 62/2011, de 9 de maio. Diário da República, 1.ª série – N.º 89.

Decreto-Lei n.º 81/2016, de 28 de novembro. Diário da República, 1.ª série – N.º 228.

Decreto-Lei n.º 65/2021, de 30 de julho. Diário da República, 1.ª série – N.º 147.

Decreto-Lei n.º 20/2022, de 28 de janeiro. Diário da República, 1.ª série – N.º 20.

Denning, P. J., & Denning, D. E. (2010). Discussing Cyber Attack. *Communications of the ACM*, *53*(9), 29-31. https://doi.org/10.1145/1810891.1810904

Despacho n.º 11491/2022, de 28 de setembro. Diário da República, 2.ª série – N.º 188.

Dias, M. (2022, fevereiro 10). Ataque à Vodafone? "É o primeiro em Portugal de origem geopolítica". *Notícias ao Minuto*. https://www.noticiasaominuto.com/tech/1930453/ataque-vodafone-o-primeiro-ataque-em-portugal-de-origem-geopoltica

Dias, M. (2023, janeiro 20). Ciberataque ao PayPal. Dados pessoais de 35 mil clientes foram roubados. *Notícias ao Minuto*.

https://www.noticiasaominuto.com/tech/2159156/ciberataque-ao-paypal-dados-pessoais-de-35-mil-clientes-foram-roubado

Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho. Jornal Oficial da União Europeia, 201/37.

Diretiva 2008/114/CE do Conselho, de 8 de dezembro. Jornal Oficial da União Europeia, 345/75.

Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho. Jornal Oficial da União Europeia, 194/1.

Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro. Jornal Oficial da União Europeia, 333/80.

Dolphin, R. R. (2004). Corporate reputation – a value creating strategy. *Corporate Governance*, *4*(3), 77-92. http://dx.doi.org/10.1108/14720700410547521

Drolet, M. (2023, 4 de janeiro). *6 Cybersecurity Trends You Can Expect In 2023*. Towerwall. https://towerwall.com/6-cybersecurity-trends-you-can-expect-in-2023/

EDP alvo de ataque informático. (2020, abril 13). *Diário de Notícias*. https://www.dn.pt/pais/edp-alvo-de-ataque-informatico-12066017.html

Eiró-Gomes, M., & Nunes, T. (2013). *Relações Públicas / Comunicação Institucional / Comunicação Corporativa: três designações para uma mesma realidade?* Em CONGRESSO SOPCOM, VIII, Lisboa, 2013 - Comunicação global, cultura e tecnologia: livro de atas (pp. 1050-1057). SOPCOM/ESCS: Lisboa.

Espírito Santo, P. (2015). *Introdução à metodologia das ciências sociais: Génese, fundamentos e problemas*. Sílabo.

European Central Bank (2018). *UNITAS Crisis communication exercise report*. Germany. https://www.ecb.europa.eu/pub/pdf/other/ecb.unitasreport201812.en.pdf

Évora, C., Pereira, C., & Mendes, R. B. (2022, abril 26). Ataque informático cancela consultas e cirurgias no Hospital Garcia de Orta. *CNN Portugal*. https://cnnportugal.iol.pt/geral/hospital-garcia-de-orta-com-dificuldades-devido-a-falha-no-sistema-informatico/20220426/6267bef70cf2ea4f0a46e109

Fisher, R., Porod, C., & Peterson, S. (2021). Motivating Employees and Organizations to Adopt a Cybersecurity-Focused Culture. *Journal of Organizational Psychology*, *21*(1), 114-131. https://doi.org/10.33423/jop.v21i1.4030

Fombrun, C. (2018). *Reputation: Realizing Value from the Corporate Image*. Harvard Business School Press. (Obra original publicada em 1996)

Fombrun, C., & Shanley, M. (1990). What's in a Name? Reputation Building and Corporate Strategy. *Academy of Management Journal*, *33*(2), 233-258. https://doi.org/10.2307/256324

Fombrun, C., & van Riel, C. (1997). The Reputational Landscape. *Corporate Reputation Review*, *1*(1-2), 5-13. 10.1057/palgrave.crr.1540008

Godoy, A. S. (1995). Pesquisa Qualitativa: tipos fundamentais. *Revista de Administração de Empresas*, *35*(3), 20-29. https://doi.org/10.1590/S0034-75901995000300004

Gonçalves, G. (2010). *Introdução à Teoria das Relações Públicas*. Porto Editora.

Gonçalves, R. S. (2019). *O fator humano da cibersegurança nas organizações*. [Dissertação de Mestrado, Instituto Superior de Economia e Gestão]. Repositório da Universidade de Lisboa. https://www.repository.utl.pt/handle/10400.5/19248

González-Herrero, A., & Pratt, C. B. (1996). An Integrated Symmetrical Model for Crisis-Communications Management. *Journal of Public Relations Research*, *8*(2), 79-105. https://doi.org/10.1207/s1532754xjprr0802_01

Goodman, M. (2015). *Future Crimes*. Transworld Publishers.

Gotsi, M., & Wilson, A. M. (2001). Corporate reputation: seeking a definition. *Corporate Communications*, *6*(1), 24-30. http://dx.doi.org/10.1108/13563280110381189

Goutam, R. K. (2015). Importance of Cyber Security. *International Journal of Computer Applications*, *111*(7), 14-17. 10.5120/19550-1250

Gray, E., & Balmer, J. (1998). Managing Corporate Image and Corporate Reputation. *Long Range Planning*, *31*(5), 695-702. https://doi.org/10.1016/S0024-6301(98)00074-0

Grunig, J. E. (2011). Public relations and strategic management: Institutionalizing organization–public relationships in contemporary society. *Central European Journal of Communication*, *4*(1), 11-31.

Grunig, J. E., & Hunt, T. (1984). *Managing Public Relations*. Lawrence Erlbaum Associates.

Grunig, L. A., Grunig, J. E., & Dozier, D. M. (2002). *Excellent Public Relations and Effective Organizations*. Lawrence Erlbaum Associates.

Grupo Super Bock alvo de ataque informático. Empresa fala em "grandes restrições". (2023, janeiro 30). *Público*. https://www.publico.pt/2023/01/30/tecnologia/noticia/grupo-super-bock-alvo-ataque-informatico-empresa-fala-restricoes-2036990

Gwebu, K. L., Wang, J., & Wang, L. (2018). The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management. *Journal of Management Information Systems*, *35*(2), 683-714. https://doi.org/10.1080/07421222.2018.1451962

Hackers atacam Estado-Maior-General das Forças Armadas e colocam documentos da NATO à venda na internet. (2022, setembro 08). *Público*. https://www.publico.pt/2022/09/08/sociedade/noticia/piratas-atacam-estadomaiorgeneral-forcas-armadas-colocam-documentos-nato-venda-internet-2019803

Harlow, R. F. (1976). Building a public relations definition. *Public Relations Review*, *2*(4), 34-42. https://doi.org/10.1016/S0363-8111(76)80022-7

Holland, A. (Coord.) (2022). *The Evolution of Cybercrime: Why the Dark Web is Supercharging the Threat Landscape and How to Fight Back*. HP Wolf Security. https://threatresearch.ext.hp.com/wp-content/uploads/2022/07/HP-Wolf-Security-Evolution-of-Cybercrime-Report.pdf

Hussain, A., Mohamed, A., & Razali, S. (2020). A Review on Cybersecurity: Challenges & Emerging Threats. *NISS2020: Proceedings of the 3rd International Conference on Networking, Information Systems & Security*, *28*, 1-7. https://doi.org/10.1145/3386723.3387847

Hutton, J. G. (1999). The Definition, Dimensions, and Domain of Public Relations. *Public Relations Review*, *25*(2), 199-214. https://doi.org/10.1016/S0363-8111(99)80162-3

Hutton, J. G. (2007). Defining the Future of Public Relations. *Sphera Pública*, (7), 45-63.

Hwang, S., Shin, D., & Kim, J. (2022). Systematic Review on Identification and Prediction of Deep Learning-Based Cyber Security Technology and Convergence Fields. *Symmetry*, *14*(4), 1-37. https://doi.org/10.3390/sym14040683

Ihlen, Ø., & van Ruler, B. (2007). How public relations works: Theoretical roots and public relations perspectives. *Public Relations Review*, *33*(3), 243-248. https://doi.org/10.1016/j.pubrev.2007.05.001

Jin, Y., & Cameron, G. T. (2007). The Effects of Threat Type and Duration on Public Relations Practitioner's Cognitive, Affective, and Conative Responses in Crisis Situations. *Journal of Public Relations Research*, *19*(3), 255-281. ttps://doi.org/10.1080/10627260701331762

Jorge, N. S. (2011). Reputação: interpretação e valor económico. In Azevedo, J., & Martins, M. L. (Eds.), *Meios digitais e indústrias criativas - Os efeitos e os desafios da globalização* (pp. 3264-3283). SOPCOM. https://sopcom2011.up.pt/media/SOPCOM_2011_Atas.pdf

Kelly, C. (2005). Data Security: A New Concern for PR Practitioners. *Public Relations Quarterly*, *50*(2), 25-26.

Kelly, P. (2023, 15 de março). *What Is the Role of Government in Cybersecurity?* GovNet. https://blog.govnet.co.uk/technology/what-is-the-role-of-government-in-cybersecurity

Kent, M. L., & Taylor, M. (2002). Toward a dialogic theory of public relations. *Public Relations Review*, *28*(1), 21-37. https://doi.org/10.1016/S0363-8111(02)00108-X

Kim, B., Johnson, K., & Park, S. (2017). Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. *Cogent Business & Management*, *4*(1), 1-15. https://doi.org/10.1080/23311975.2017.1354525

Kim, N., & Lee, S. (2018). Cybersecurity Breach and Crisis Response: An Analysis of Organizations' Official Statements in the United States and South Korea. *International Journal of Business Communication*, *58*(4), 1-22. https://doi.org/10.1177/232948841877703

Knight, R., & Nurse, J. (2020). A Framework for Effective Corporate Communication after Cyber Security Incidents. *Computers & Security Journal*, *99*, 1-34. https://doi.org/10.1016/j.cose.2020.102036

Kuipers, S., & Schonheit, M. (2021). Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises. *Corporate Reputation Review*, *25*(3), 176-197. 10.1057/s41299-021-00121-9

Laboratórios Germano de Sousa alvo de ciberataque. (2022, fevereiro 10). *RTP*. https://www.rtp.pt/noticias/pais/laboratorios-germano-de-sousa-alvo-de-ciberataque_n1383469

Lange, D., Lee, P. M., & Dai, Y. (2011). Organizational Reputation: A Review. *Journal of Management*, *37*(1), 153-184. https://doi.org/10.1177/0149206310390963

Lei n.º 109/2009, de 15 de setembro. Diário da República, 1.ª série – N.º 179.

Lei n.º 46/2018, de 13 de agosto. Diário da República, 1.ª série – N.º 155.

Lella, I., Tsekmezoglou, E., Theocharidou, M., Magonara, E., Malatras, A., Naydenov, R. S., & Ciobanu, C. (Eds.) (2023). *ENISA Threat Landscape 2023*. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Lewis, S. (2001). Measuring corporate reputation. *Corporate Communications*, *6*(1), 31-35. 10.1108/13563280110381198

Lourenço, R. P. (Coord.) (2021). *Cibersegurança em Portugal: Políticas Públicas*. Observatório de Cibersegurança. https://www.cncs.gov.pt/docs/relatorio-politicaspublicas2021-observatoriociberseguranca-cncs.pdf

Lusa, A. (2020, abril 16). Altice alvo de ciberataque garante que consequências foram "praticamente nulas". *ECO*. https://eco.sapo.pt/2020/04/16/altice-alvo-de-ciberataque-garante-que-consequencias-foram-praticamente-nulas/

Lusa, A. (2022a, maio 25). Agência Lusa alvo de novo ataque informático. *Jornal de Negócios*. https://www.jornaldenegocios.pt/empresas/media/detalhe/agencia-lusa-alvo-de-novo-ataque-informatico

Lusa, A. (2022b, dezembro 16). Amnistia Internacional no Canadá diz que foi alvo de ciberataque chinês. *Notícias ao Minuto*. https://www.noticiasaominuto.com/tech/2127092/amnistia-internacional-no-canada-diz-que-foi-alvo-de-ciberataque-chines

Lusa, A.. (2022c, dezembro 26). Ucrânia acusa Rússia de realizar mais de 4500 ciberataques em 2022. *Diário de Notícias*. https://www.dn.pt/internacional/ucrania-acusa-russia-de-realizar-mais-de-4500-ciberataques-em-2022-15553519.html

Lusa, A. (2023a, janeiro 29). Ciberataques: Direção-Geral da Saúde foi alvo de ataque mas 'site' está funcional. *Observador*. https://observador.pt/2023/01/29/ciberataques-direcao-geral-da-saude-foi-alvo-de-ataque-mas-site-esta-funcional/

Lusa, A. (2023b, fevereiro 05). Ciberataque "massivo" em Itália provoca problemas informáticos. *Observador*. https://observador.pt/2023/02/05/ciberataque-massivo-em-italia-provoca-problemas-informaticos/

Lusa, A. (2023c, fevereiro 08). Global Media Group alvo de ciberataque liderado por pirata informático português. *CNN Portugal*. https://cnnportugal.iol.pt/global-media/marco-galinha/sites-da-global-media-alvo-de-ciberataque/20230208/63e42def0cf2c84d7fc70fad

Lusa, A. (2023d, fevereiro 13). Grupo Visabeira com sede em Viseu alvo de ataque ao sistema informático. *Observador*. https://observador.pt/2023/02/13/grupo-visabeira-com-sede-em-viseu-alvo-de-ataque-ao-sistema-informatico/

Lusa, A. (2023e, abril 06). Ministério da Economia com 85% do impacto do ciberataque restabelecido. *RTP*. https://www.rtp.pt/noticias/economia/ministerio-da-economia-com-85-do-impacto-do-ciberataque-restabelecido_n1478002

Lusa, A. (2023f, agosto 06). Ciberataque força suspensão de atividade clínica no Serviço de Saúde da Madeira. *Público*. https://www.publico.pt/2023/08/06/tecnologia/noticia/ciberataque-forca-suspensao-actividade-clinica-servico-saude-madeira-2059423

Ma, L., & Zhan, M. (2016). Effects of attributed responsibility and response strategies on organizational reputation: A meta-analysis of situational crisis communication theory research. *Journal of Public Relations Research*, *28*(2), 102-119. https://doi.org/10.1080/1062726X.2016.1166367

Machado, A., Ferreira, B., & Correia, G. (2022, janeiro 02). Sites do jornal Expresso e da SIC hackeados com pedidos de resgate pelos piratas informáticos. *Observador*. https://observador.pt/2022/01/02/sites-do-jornal-expresso-e-da-sic-hackeados-com-pedidos-de-resgate-pelos-piratas-informaticos/

Mahon, J. F. (2002). Corporate Reputation: A Research Agenda Using Strategy and Stakeholder Literature. *Business & Society*, *41*(4), 415-445. https://doi.org/10.1177/0007650302238776

Manley, B., & McIntire, D. (2020). *A Guide to Effective Incident Management Communications*. Carnegie Mellon University. https://apps.dtic.mil/sti/pdfs/AD1117526.pdf

Marques, A. C. (2022, março 30). Grupo Sonae foi alvo de ataque informático nas últimas horas. *Observador*. https://observador.pt/2022/03/30/grupo-sonae-foi-alvo-de-ataque-informatico-nas-ultimas-horas/

Martins, B. B. (2022). *Comunicação de crise através das Redes Sociais: o caso da Vodafone*. [Dissertação de Mestrado, Faculdade de Artes e Letras]. uBibliorum: Repositório Digital da UBI. https://ubibliorum.ubi.pt/handle/10400.6/13122

Mendes, A. M. (2013). Reputação organizacional e Relações Públicas: contributos para o esclarecimento da hierarquia entre os conceitos. *Comunicação Pública*, *8*(13), 25-39. https://doi.org/10.4000/cp.483

Mesquita, P. (2022, setembro 28). Ciberataques. "Grau de preparação ainda insuficiente" em Portugal. *Rádio Renascença*. https://rr.sapo.pt/noticia/pais/2022/09/28/ciberataques-grau-de-preparacaoainda-insuficiente-em-portugal/301542

Michaelson, D., & Stacks, D. W. (2014). *A Professional and Practitioner's Guide to Public Relations Research, Measurement, and Evaluation*. Business Expert Press.

Ministry of Interior, Republic of Serbia (2019). *Cyberattacks and crisis communications: a matter of reputation*. Kaspersky Lab. https://media.kaspersky.com/en/business-security/case-studies/Kaspersky%20Incident%20Communications%20-%20Cyberattacks%20and%20crisis%20communication.pdf

Miranda, A. (2022, fevereiro 08). Ciberataque à Vodafone "teve origem num ato terrorista e criminoso". *CNN Portugal*. https://cnnportugal.iol.pt/geral/ciberataque-a-vodafone-teve-origem-num-ato-terrorista-e-criminoso-a-rede/20220208/6202597d0cf21847f0a9d3c3

Monteiro, H. (2022, novembro 30). Ciberataques. Fuga de dados atinge mais de 2,2 milhões de utilizadores do Whatsapp em Portugal. *Rádio Renascença*.

https://rr.sapo.pt/noticia/mundo/2022/11/30/ciberataques-fuga-de-dados-atinge-mais-de-22-milhoes-de-utilizadores-do-whatsapp-em-portugal/310168/

Mpholo, L. (2022, 22 de agosto*). How businesses can use PR (Public Relations) as part of their cyber security management*. Bizcommunity. https://www.bizcommunity.com/Article/196/18/230759.html

Myers, C. (2021). *Public Relations History: Theory, Practice, and Profession*. Routledge.

Narendra, M. (2022, maio 03). A importância da gestão de crise na resposta a ciberataques. *Dinheiro Vivo*. https://www.dinheirovivo.pt/opiniao/a-importancia-da-gestao-de-crise-na-resposta-a-ciberataques-14822037.html

Neutel, H. (2022, outubro 03). BCP alvo de ciberataque. Situação já a normalizar, diz banco. *Jornal de Negócios*. https://www.jornaldenegocios.pt/empresas/banca---financas/detalhe/bcp-alvo-de-ciberataque-situacao-ja-a-normalizar-diz-banco

Nunes, F. (2022, setembro 22). Ciberataque à TAP: o que disse a empresa (e o que aconteceu depois). *ECO*. https://eco.sapo.pt/2022/09/22/ciberataque-a-tap-o-que-disse-a-empresa-e-o-que-aconteceu-depois/

Pande, J. (2017). *Introduction to Cyber Security*. Uttarakhand Open University.

Park, H. (2016). Exploring effective crisis response strategies. *Public Relations Review*, *43*(1), 190-192. https://doi.org/10.1016/j.pubrev.2016.12.001

Pearson, C. M., & Clair, J. A. (1998). Reframing Crisis Management. *Academy of Management Review*, *23*(1), 59-76. https://doi.org/10.2307/259099

Pearson, C. M., & Mitroff, I. I. (1993). From crisis prone to crisis prepared: a framework for crisis management. *Academy of Management Executive*, *7*(1), 48-59. https://doi.org/10.5465/ame.1993.9409142058

Rao, A., Hurley, B., Bhat, R., Iyer, A., & Downey, E. (Coords.) (2022). *Tech Trends 2023*. Deloitte. https://www2.deloitte.com/content/dam/insights/articles/us175897_tech-trends-2023/DI_tech-trends-2023.pdf

Regulamento n.º 183/2022, de 21 de fevereiro. Diário da República, 2.ª série – N.º 36.

Regulamento (EU) 2014/910 do Parlamento Europeu e do Conselho, de 23 de julho. Jornal Oficial da União Europeia, 257/73.

Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril. Jornal Oficial da União Europeia, 119/1.

Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril. Jornal Oficial da União Europeia, 151/15.

Resolução do Conselho de Ministros n.º 12/2012, de 7 de fevereiro. Diário da República, 1.ª sério – N.º 27.

Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho. Diário da República, 1.ª série – N.º 113.

Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho. Diário da República, 1.ª série – N.º 108.

Resolução do Conselho de Ministro n.º 106/2022, de 2 de novembro. Diário da República, 1.ª série – N.º 211.

Roberts, P. W., & Dowling, G. R. (2002). Corporate Reputation and Sustained Superior Financial Performance. *Strategic Management Journal*, *23*(12), 1077-1093. https://doi.org/10.1002/smj.274

Santos, S. Q. (2021). *Comunicação de Crises em Cibersegurança*. [Dissertação de Mestrado, Faculdade de Ciências Sociais e Humanas]. Repositório Universidade Nova. https://run.unl.pt/handle/10362/130218

Sapriel, C. (2021). Managing stakeholder communication during a cyber crisis. *Journal of Cyber Security and Mobility*, *4*(4), 1-8.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*, *12*(2), 53-74. https://doi.org/10.15394/jdfsl.2017.1476

Schnietz, K. E., & Epstein, M. J. (2005). Exploring the Financial Value of a Reputation for Corporate Social Responsibility During a Crisis. *Corporate Reputation Review*, *7*(4), 327-345. 10.1057/PALGRAVE.CRR.1540230

Schreier, M. (2012). *Qualitative content analysis in practice*. SAGE Publications.

Schwaiger, M. (2004). Components and Parameters of Corporate Reputation - An Empirical Study. *Schmalenbach Business Review*, *56*, 46-71. https://ssrn.com/abstract=555102

Sebastião, S. P. (2012). Relações públicas: a comunicação, as organizações e a sociedade. *Comunicação Pública*, *7*(12), 23-42. https://doi.org/10.4000/cp.112

Seeger, M. W. (2006). Best Practices in Crisis Communication: An Expert Panel Process. *Journal of Applied Communication Research*, *34*(3), 232-244. https://doi.org/10.1080/00909880600769944

Seidman, I. (2006). *Interviewing as Qualitative Research*. Teachers College Press.

Séneca, H. (2022a, novembro 23). Ciberataque à Segurança Social "visava a destruição" de bases de dados que são das mais valiosas para Portugal. *Expresso*. https://expresso.pt/sociedade/ciencia/2022-11-23-Ciberataque-a-Seguranca-Social-visava-a-destruicao-de-bases-de-dados-que-sao-das-mais-valiosas-para-Portugal-0217bbfa

Séneca, H. (2022b, dezembro 15). INEM e Universidade Católica foram alvo de ciberataques. *Expresso*. https://expresso.pt/sociedade/ciencia/2022-12-15-INEM-e-Universidade-Catolica-foram-alvo-de-ciberataques-5991fe8a

Séneca, H. (2023, junho 22). Grupo Luís Simões alvo de ciberataque reivindicado na Dark Web. *Expresso*. https://expresso.pt/economia/economia_tecnologia/2023-06-22-Grupo-Luis-Simoes-alvo-de-ciberataque-reivindicado-na-Dark-Web-c02ccb05

Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. Elsevier.

Silva, F. C. (2022, março 30). Ronin Network sofre o maior roubo da história do mercado cripto. *Jornal de Negócios*. https://www.jornaldenegocios.pt/mercados/criptoativos/detalhe/ronin-network-sofre-o-maior-roubo-da-historia-do-mercado-cripto

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Sites do Sporting e FC Porto alvo de ataques informáticos. (2022b, setembro 15). *Diário de Notícias*. https://www.dn.pt/desporto/site-do-sporting-alvo-de-ataque-informatico-15166802.html

Soares, M. R. (2020, dezembro 20). O que se sabe sobre o maior ataque informático ao Governo dos EUA. *RTP*. https://www.rtp.pt/noticias/mundo/o-que-se-sabe-sobre-o-maior-ataque-informatico-ao-governo-dos-eua_n1284002

Srinivas, J., Das, A. K., & Kumar, N. (2018). Government regulations in cyber security: Framework, standards and recommendation. *Future Generation Computer Systems, 92*, 1-13. https://doi.org/10.1016/j.future.2018.09.063

Sturges, D. L. (1994). Communicating through Crisis: A Strategy for Organizational Survival. *Management Communication Quarterly*, *7*(3), 297-316. https://doi.org/10.1177/0893318994007003004

Tam, L., Kim, J., Grunig, J. E., Hall, J. A., & Swerling, J. (2020). In search of communication excellence: Public relations' value, empowerment, and structure in strategic management. *Journal of Marketing Communications*, *28*(2), 183-206. https://doi.org/10.1080/13527266.2020.1851286

Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks*. Prentice Hall.

Tench, R., & Yeomans, L. (2009). *Exploring Public Relations*. Prentice Hall.

Theaker, A. (2012). *The Public Relations Handbook*. Routledge.

Threat Landscape Report 2023. (2023). S21sec. https://www.s21sec.com/wp-content/uploads/2023/07/S21sec_Thales_ThreatLandscapeReport_2023_EN.pdf

Top 7 Trends Shaping Digital Transformation in 2023. (2022). MuleSoft. https://www.mulesoft.com/lp/reports/top-digital-transformation-trends

van Riel, C., & Fombrun, C. (2007). *Essentials of Corporate Communication*. Routledge.

Verčič, D., van Ruler, B., Bütschi, G., & Flodin, B. (2001). On the definition of public relations: a European view. *Public Relations Review*, *27*(4), 373-387. https://doi.org/10.1016/S0363-8111(01)00095-9

von Solms, B., & von Solms, R. (2018). Cyber Security and Information Security – What goes where? *Information & Computer Security*, *26*(1), 1-9. https://doi.org/10.1108/ICS-04-2017-0025

von Solms, R., & van Niekerk (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Wang, P., & Park, S. (2017). Communication in Cybersecurity: a public communication model for business data breach incident handling. *Issues in Information Systems*, *18*(2), 136-147. https://doi.org/10.48009/2_iis_2017_136-147

Wartick, S. L. (2002). Measuring Corporate Reputation: Definition and Data. *Business & Society*, *41*(4), 371-392. https://doi.org/10.1177/0007650302238774

Weigelt, K., & Camerer, C. (1988). Reputation and Corporate Strategy: A Review of Recent Theory and Applications. *Strategic Management Journal*, *9*(5), 443-454. https://doi.org/10.1002/smj.4250090505

Weiner, B. (1985). An Attributional Theory of Achievement Motivation and Emotion. *Psychological Review*, *92*(4), 548-573. https://doi.org/10.1037/0033-295X.92.4.548

Wilcox, D. L., Cameron, G. T., & Xifra, J. (2012). *Relaciones Públicas: Estrategias y tácticas.* Pearson Education.

Apêndices

Apêndice 1: Protocolos de investigação

- Rui Duro

PROTOCOLO DE INVESTIGAÇÃO | DISSERTAÇÃO DE MESTRADO

Esta entrevista é realizada no âmbito do trabalho de dissertação para a obtenção do grau de Mestre em Gestão Estratégica das Relações Públicas, de Sara Alexandra Gaspar Antunes, pela ESCS – Escola Superior de Comunicação Social, sob a orientação do Professor Doutor Nuno da Silva Jorge.

O referido trabalho explora o papel da comunicação de crise em situação de ciberataque. Por forma a aprofundar o tema e a sua compreensão, será realizada a presente entrevista, que terá uma duração aproximada de 30 minutos.

O estudo decorrerá segundo os princípios éticos internacionais, sendo que a informação recolhida se destina exclusivamente para os fins académicos desta investigação, não lhe podendo ser dada outra utilização sem o consentimento escrito do participante.

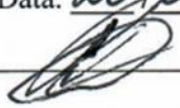
Por motivos de rigor metodológico, a entrevista será gravada em formato áudio. Esta gravação será destruída após transcrição dos dados e serve unicamente a função de manter a fidelidade da informação expressa pelos participantes. Uma cópia da transcrição da entrevista será disponibilizada para o seu conhecimento. Importa ressalvar que a sua participação é voluntária e apenas se realizará mediante o seu consentimento.

A sua participação é essencial para a execução deste trabalho. Obrigada pela sua colaboração.

Termo de Participação

Após ter lido e compreendido o protocolo de investigação, confirmo a minha participação, em função dos termos acima mencionados.

Data: 26/6/2023

Rubrica: 

- Mauro Almeida

PROTOCOLO DE INVESTIGAÇÃO | DISSERTAÇÃO DE MESTRADO

Esta entrevista é realizada no âmbito do trabalho de dissertação para a obtenção do grau de Mestre em Gestão Estratégica das Relações Públicas, de Sara Alexandra Gaspar Antunes, pela ESCS – Escola Superior de Comunicação Social, sob a orientação do Professor Doutor Nuno da Silva Jorge.

O referido trabalho explora o papel da comunicação de crise em situação de ciberataque. Por forma a aprofundar o tema e a sua compreensão, será realizada a presente entrevista, que terá uma duração aproximada de 30 minutos.

O estudo decorrerá segundo os princípios éticos internacionais, sendo que a informação recolhida se destina exclusivamente para os fins académicos desta investigação, não lhe podendo ser dada outra utilização sem o consentimento escrito do participante.

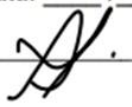
Por motivos de rigor metodológico, a entrevista será gravada em formato áudio. Esta gravação será destruída após transcrição dos dados e serve unicamente a função de manter a fidelidade da informação expressa pelos participantes. Uma cópia da transcrição da entrevista será disponibilizada para o seu conhecimento. Importa ressalvar que a sua participação é voluntária e apenas se realizará mediante o seu consentimento.

A sua participação é essencial para a execução deste trabalho. Obrigada pela sua colaboração.

Termo de Participação

Após ter lido e compreendido o protocolo de investigação, confirmo a minha participação, em função dos termos acima mencionados.

Data: 27 / 06 / 2023

Rubrica: 

- Pedro Mendonça

PROTOCOLO DE INVESTIGAÇÃO | DISSERTAÇÃO DE MESTRADO

Esta entrevista é realizada no âmbito do trabalho de dissertação para a obtenção do grau de Mestre em Gestão Estratégica das Relações Públicas, de Sara Alexandra Gaspar Antunes, pela ESCS – Escola Superior de Comunicação Social, sob a orientação do Professor Doutor Nuno da Silva Jorge.

O referido trabalho explora o papel da comunicação de crise em situação de ciberataque. Por forma a aprofundar o tema e a sua compreensão, será realizada a presente entrevista, que terá uma duração aproximada de 30 minutos.

O estudo decorrerá segundo os princípios éticos internacionais, sendo que a informação recolhida se destina exclusivamente para os fins académicos desta investigação, não lhe podendo ser dada outra utilização sem o consentimento escrito do participante.

Por motivos de rigor metodológico, a entrevista será gravada em formato áudio. Esta gravação será destruída após transcrição dos dados e serve unicamente a função de manter a fidelidade da informação expressa pelos participantes. Uma cópia da transcrição da entrevista será disponibilizada para o seu conhecimento. Importa ressalvar que a sua participação é voluntária e apenas se realizará mediante o seu consentimento.

A sua participação é essencial para a execução deste trabalho. Obrigada pela sua colaboração.

Termo de Participação

Após ter lido e compreendido o protocolo de investigação, confirmo a minha participação, em função dos termos acima mencionados.

Data: ____ /____/ _____

Rubrica: _____

Assinado por: **Pedro Filipe Xavier Mendonça**
Num. de Identificação: 11406069
Data: 2023.07.31 16:25:40+01'00'

CHAVE MÓVEL

- António Gameiro Marques

PROTOCOLO DE INVESTIGAÇÃO | DISSERTAÇÃO DE MESTRADO

Esta entrevista é realizada no âmbito do trabalho de dissertação para a obtenção do grau de Mestre em Gestão Estratégica das Relações Públicas, de Sara Alexandra Gaspar Antunes, pela ESCS – Escola Superior de Comunicação Social, sob a orientação do Professor Doutor Nuno da Silva Jorge.

O referido trabalho explora o papel da comunicação de crise em situação de ciberataque. Por forma a aprofundar o tema e a sua compreensão, será realizada a presente entrevista, que terá uma duração aproximada de 30 minutos.

O estudo decorrerá segundo os princípios éticos internacionais, sendo que a informação recolhida se destina exclusivamente para os fins académicos desta investigação, não lhe podendo ser dada outra utilização sem o consentimento escrito do participante.

Por motivos de rigor metodológico, a entrevista será gravada em formato áudio. Esta gravação será destruída após transcrição dos dados e serve unicamente a função de manter a fidelidade da informação expressa pelos participantes. Uma cópia da transcrição da entrevista será disponibilizada para o seu conhecimento. Importa ressalvar que a sua participação é voluntária e apenas se realizará mediante o seu consentimento.

A sua participação é essencial para a execução deste trabalho. Obrigada pela sua colaboração.

Termo de Participação

Após ter lido e compreendido o protocolo de investigação, confirmo a minha participação, em função dos termos acima mencionados.

Data: ____ /____/ _____

Rubrica: _____

António José Gameiro Marques

Digitally signed by António José Gameiro Marques
Date: 2023.07.05 09:50:54 +01'00'

- Pedro Verdelho

PROTOCOLO DE INVESTIGAÇÃO | DISSERTAÇÃO DE MESTRADO

Esta entrevista é realizada no âmbito do trabalho de dissertação para a obtenção do grau de Mestre em Gestão Estratégica das Relações Públicas, de Sara Alexandra Gaspar Antunes, pela ESCS – Escola Superior de Comunicação Social, sob a orientação do Professor Doutor Nuno da Silva Jorge.

O referido trabalho explora o papel da comunicação de crise em situação de ciberataque. Por forma a aprofundar o tema e a sua compreensão, será realizada a presente entrevista, que terá uma duração aproximada de 30 minutos.

O estudo decorrerá segundo os princípios éticos internacionais, sendo que a informação recolhida se destina exclusivamente para os fins académicos desta investigação, não lhe podendo ser dada outra utilização sem o consentimento escrito do participante.

Por motivos de rigor metodológico, a entrevista será gravada em formato áudio. Esta gravação será destruída após transcrição dos dados e serve unicamente a função de manter a fidelidade da informação expressa pelos participantes. Uma cópia da transcrição da entrevista será disponibilizada para o seu conhecimento. Importa ressalvar que a sua participação é voluntária e apenas se realizará mediante o seu consentimento.

A sua participação é essencial para a execução deste trabalho. Obrigada pela sua colaboração.

Termo de Participação

Após ter lido e compreendido o protocolo de investigação, confirmo a minha participação, em função dos termos acima mencionados.

Data: 18/07/2023

(Pedro Verdelho)

- Duarte Freitas

PROTOCOLO DE INVESTIGAÇÃO | DISSERTAÇÃO DE MESTRADO

Esta entrevista é realizada no âmbito do trabalho de dissertação para a obtenção do grau de Mestre em Gestão Estratégica das Relações Públicas, de Sara Alexandra Gaspar Antunes, pela ESCS – Escola Superior de Comunicação Social, sob a orientação do Professor Doutor Nuno da Silva Jorge.

O referido trabalho explora o papel da comunicação de crise em situação de ciberataque. Por forma a aprofundar o tema e a sua compreensão, será realizada a presente entrevista, que terá uma duração aproximada de 30 minutos.

O estudo decorrerá segundo os princípios éticos internacionais, sendo que a informação recolhida se destina exclusivamente para os fins académicos desta investigação, não lhe podendo ser dada outra utilização sem o consentimento escrito do participante.

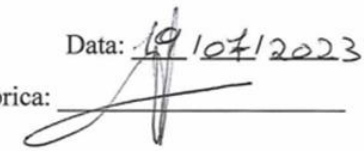
Por motivos de rigor metodológico, a entrevista será gravada em formato áudio. Esta gravação será destruída após transcrição dos dados e serve unicamente a função de manter a fidelidade da informação expressa pelos participantes. Uma cópia da transcrição da entrevista será disponibilizada para o seu conhecimento. Importa ressalvar que a sua participação é voluntária e apenas se realizará mediante o seu consentimento.

A sua participação é essencial para a execução deste trabalho. Obrigada pela sua colaboração.

Termo de Participação

Após ter lido e compreendido o protocolo de investigação, confirmo a minha participação, em função dos termos acima mencionados.

Data: 19/07/2023

Rubrica: 

- Alexandra Abreu Loureiro

PROTOCOLO DE INVESTIGAÇÃO | DISSERTAÇÃO DE MESTRADO

Esta entrevista é realizada no âmbito do trabalho de dissertação para a obtenção do grau de Mestre em Gestão Estratégica das Relações Públicas, de Sara Alexandra Gaspar Antunes, pela ESCS – Escola Superior de Comunicação Social, sob a orientação do Professor Doutor Nuno da Silva Jorge.

O referido trabalho explora o papel da comunicação de crise em situação de ciberataque. Por forma a aprofundar o tema e a sua compreensão, será realizada a presente entrevista, que terá uma duração aproximada de 30 minutos.

O estudo decorrerá segundo os princípios éticos internacionais, sendo que a informação recolhida se destina exclusivamente para os fins académicos desta investigação, não lhe podendo ser dada outra utilização sem o consentimento escrito do participante.

Por motivos de rigor metodológico, a entrevista será gravada em formato áudio. Esta gravação será destruída após transcrição dos dados e serve unicamente a função de manter a fidelidade da informação expressa pelos participantes. Uma cópia da transcrição da entrevista será disponibilizada para o seu conhecimento. Importa ressalvar que a sua participação é voluntária e apenas se realizará mediante o seu consentimento.

A sua participação é essencial para a execução deste trabalho. Obrigada pela sua colaboração.

Termo de Participação

Após ter lido e compreendido o protocolo de investigação, confirmo a minha participação, em função dos termos acima mencionados.

Data: ____ /____/ _____

Rubrica: _____

Alexandra Abreu Loureiro
Partner, Head of Portugal
Brunswick Group LLP
16 Lincoln's Inn Fields
London WC2A 3RD
+447889591836
www.brunswickgroup.com

- Paula Ramos

PROTOCOLO DE INVESTIGAÇÃO | DISSERTAÇÃO DE MESTRADO

Esta entrevista é realizada no âmbito do trabalho de dissertação para a obtenção do grau de Mestre em Gestão Estratégica das Relações Públicas, de Sara Alexandra Gaspar Antunes, pela ESCS – Escola Superior de Comunicação Social, sob a orientação do Professor Doutor Nuno da Silva Jorge.

O referido trabalho explora o papel da comunicação de crise em situação de ciberataque. Por forma a aprofundar o tema e a sua compreensão, será realizada a presente entrevista, que terá uma duração aproximada de 30 minutos.

O estudo decorrerá segundo os princípios éticos internacionais, sendo que a informação recolhida se destina exclusivamente para os fins académicos desta investigação, não lhe podendo ser dada outra utilização sem o consentimento escrito do participante.

Por motivos de rigor metodológico, a entrevista será gravada em formato áudio. Esta gravação será destruída após transcrição dos dados e serve unicamente a função de manter a fidelidade da informação expressa pelos participantes. Uma cópia da transcrição da entrevista será disponibilizada para o seu conhecimento. Importa ressalvar que a sua participação é voluntária e apenas se realizará mediante o seu consentimento.

A sua participação é essencial para a execução deste trabalho. Obrigada pela sua colaboração.

Termo de Participação

Após ter lido e compreendido o protocolo de investigação, confirmo a minha participação, em função dos termos acima mencionados.

Data: 31/07/2023

Rubrica: PaulaRamosPaula

- António Borges

PROTOCOLO DE INVESTIGAÇÃO | DISSERTAÇÃO DE MESTRADO

Esta entrevista é realizada no âmbito do trabalho de dissertação para a obtenção do grau de Mestre em Gestão Estratégica das Relações Públicas, de Sara Alexandra Gaspar Antunes, pela ESCS – Escola Superior de Comunicação Social, sob a orientação do Professor Doutor Nuno da Silva Jorge.

O referido trabalho explora o papel da comunicação de crise em situação de ciberataque. Por forma a aprofundar o tema e a sua compreensão, será realizada a presente entrevista, que terá uma duração aproximada de 30 minutos.

O estudo decorrerá segundo os princípios éticos internacionais, sendo que a informação recolhida se destina exclusivamente para os fins académicos desta investigação, não lhe podendo ser dada outra utilização sem o consentimento escrito do participante.

Por motivos de rigor metodológico, a entrevista será gravada em formato áudio. Esta gravação será destruída após transcrição dos dados e serve unicamente a função de manter a fidelidade da informação expressa pelos participantes. Uma cópia da transcrição da entrevista será disponibilizada para o seu conhecimento. Importa ressalvar que a sua participação é voluntária e apenas se realizará mediante o seu consentimento.

A sua participação é essencial para a execução deste trabalho. Obrigada pela sua colaboração.

Termo de Participação

Após ter lido e compreendido o protocolo de investigação, confirmo a minha participação, em função dos termos acima mencionados.

Data: ____/____/_____

Rubrica: _____

Assinado por: **António Eduardo Simões Borges**
Num. de Identificação: 11807731
Data: 2023.08.25 10:20:02+01'00'

- Rui Cabrita

PROTOCOLO DE INVESTIGAÇÃO | DISSERTAÇÃO DE MESTRADO

Esta entrevista é realizada no âmbito do trabalho de dissertação para a obtenção do grau de Mestre em Gestão Estratégica das Relações Públicas, de Sara Alexandra Gaspar Antunes, pela ESCS – Escola Superior de Comunicação Social, sob a orientação do Professor Doutor Nuno da Silva Jorge.

O referido trabalho explora o papel da comunicação de crise em situação de ciberataque. Por forma a aprofundar o tema e a sua compreensão, será realizada a presente entrevista, que terá uma duração aproximada de 30 minutos.

O estudo decorrerá segundo os princípios éticos internacionais, sendo que a informação recolhida se destina exclusivamente para os fins académicos desta investigação, não lhe podendo ser dada outra utilização sem o consentimento escrito do participante.

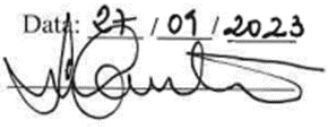
Por motivos de rigor metodológico, a entrevista será gravada em formato áudio. Esta gravação será destruída após transcrição dos dados e serve unicamente a função de manter a fidelidade da informação expressa pelos participantes. Uma cópia da transcrição da entrevista será disponibilizada para o seu conhecimento. Importa ressalvar que a sua participação é voluntária e apenas se realizará mediante o seu consentimento.

A sua participação é essencial para a execução deste trabalho. Obrigada pela sua colaboração.

Termo de Participação

Após ter lido e compreendido o protocolo de investigação, confirmo a minha participação, em função dos termos acima mencionados.

Data: 27 / 09 / 2023

Rubrica: 

- Anabela Lopes Simões

PROTOCOLO DE INVESTIGAÇÃO | DISSERTAÇÃO DE MESTRADO

Esta entrevista é realizada no âmbito do trabalho de dissertação para a obtenção do grau de Mestre em Gestão Estratégica das Relações Públicas, de Sara Alexandra Gaspar Antunes, pela ESCS – Escola Superior de Comunicação Social, sob a orientação do Professor Doutor Nuno da Silva Jorge.

O referido trabalho explora o papel da comunicação de crise em situação de ciberataque. Por forma a aprofundar o tema e a sua compreensão, será realizada a presente entrevista, que terá uma duração aproximada de 30 minutos.

O estudo decorrerá segundo os princípios éticos internacionais, sendo que a informação recolhida se destina exclusivamente para os fins académicos desta investigação, não lhe podendo ser dada outra utilização sem o consentimento escrito do participante.

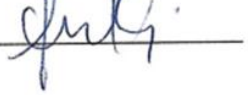
Por motivos de rigor metodológico, a entrevista será gravada em formato áudio. Esta gravação será destruída após transcrição dos dados e serve unicamente a função de manter a fidelidade da informação expressa pelos participantes. Uma cópia da transcrição da entrevista será disponibilizada para o seu conhecimento. Importa ressalvar que a sua participação é voluntária e apenas se realizará mediante o seu consentimento.

A sua participação é essencial para a execução deste trabalho. Obrigada pela sua colaboração.

Termo de Participação

Após ter lido e compreendido o protocolo de investigação, confirmo a minha participação, em função dos termos acima mencionados.

Data: 30/10/23

Rubrica: 

Apêndice 2: Entrevista Rui Duro

<u>Q1: Gostaria que o Rui me falasse um pouco sobre a sua experiência na área da Cibersegurança.</u>

Rui Duro (RD): Eu ando nisto já há praticamente 30 anos. Eu comecei a trabalhar nesta área como cliente. Trabalhei num centro de informática no Instituto Superior Técnico e, já nessa altura, era uma área à qual estávamos ligados, porque tivemos, no longínquo ano de 90 e poucos, alguns ataques, embora muito rudimentares comparados com aquilo que se faz agora. Mas já tínhamos

alguns problemas e, na altura, fez-se lá no Instituto talvez das primeiras conferências sobre cibersegurança que houve no país. Em 2000, saí e fui trabalhar para o integrador, ou seja, são aquelas empresas que instalam normalmente nos clientes finais as soluções. Portanto, instalei muitas das soluções que, ainda hoje, estão em muitas das grandes empresas em Portugal. Passei depois para uma fase de consultoria no grupo Portugal Telecom, ligado sempre à cibersegurança. E há 13 anos, sou o responsável da *Check Point Software Technologies* em Portugal. É um fabricante que eu vim sempre a acompanhar e acabei por vir cá parar. Portanto, diria que o meu percurso ligado à cibersegurança tem 30 anos… ligado como cliente, como técnico, depois como consultoria, desenvolver muitas das soluções no grupo Portugal Telecom que suportam grandes ligações em Portugal e agora ligado mesmo ao fabricante que vende a grande maioria destas soluções.

Q2: Passemos, então, à parte do meu objeto de estudo. Gostaria que o Rui começasse por me falar sobre a evolução dos ciberataques em Portugal. Ou seja, como é que surgiram e de que forma evoluíram até aos dias de hoje.

RD: Se calhar começo pelo contrário. Neste momento, há um pouco aquela ideia – e sempre houve esta ideia – de que nós estávamos aqui num cantinho do mundo e que ninguém queria nada de nós. E muitas vezes acontece que muitas empresas têm também essa ideia, do tipo "eu não tenho nada que interesse aos cibercriminosos, eu não tenho valor, eu não tenho informação confidencial". Em Portugal, havia um pouco essa ideia e essa ideia não pode estar mais errada, porque se nós fizermos uma análise da tendência de ataques ou do tipo de ataques que são feitos a nível mundial e se colocarmos uma linha paralela que representa Portugal, ela tem exatamente a mesma configuração e a mesma oscilação. Nós estamos integrados num mundo global e, hoje, os ataques em Portugal são iguais e com a mesma dimensão daqueles que ocorrem nos Estados Unidos, ou em França ou na Espanha, ou em qualquer lado do mundo. Isto obviamente tem a ver com a evolução da *Internet* e da globalização. No passado, era ligeiramente diferente. De facto, muitas vezes Portugal não era o país mais atacado, mas eramos dos países que participava mais nos ataques, devido à baixa proteção e ao pouco cuidado que há por parte das empresas em Portugal. Então, as empresas portuguesas tinham os seus sistemas – mais os PC's, não os sistemas de grande porte – reféns e participávamos naqueles ataques de *spam*, nos ataques de *denial-of-service*, nos ataques de *phishing*… Porque, apesar de não haver grandes ataques a companhias portuguesas – isto num passado mais longínquo, não num passado recente –, havia muitas máquinas em Portugal infetadas, que eram utilizadas para fazer ataques noutras partes do mundo. Hoje, não estamos exatamente ao mesmo nível, nem o mesmo número de invenções, nem o mesmo número de ataques são feitos às empresas portuguesas.

Q3: Sendo assim, comparado com o panorama mundial, qual considera ser o grau de preparação das empresas portuguesas atualmente?

RD: Em Portugal, sempre houve dois pelotões e continua a haver esses mesmos dois pelotões. De forma transversal, as grandes instituições – quer sejam privadas, quer sejam públicas – estão normalmente mais preparadas, têm cuidado, estabelecem orçamentos e, mesmo assim, não evitam ser atacadas, como todos os casos que conhecemos, que são normalmente a grandes instituições. No caso das mais pequenas – quer sejam privadas ou públicas e, no caso das públicas, estamos a falar das Câmaras –, por norma, não há sensibilidade para a temática, logo não há orçamento e, automaticamente, não há três coisas que são fundamentais: formação das pessoas, recursos humanos dedicados e com *know-how* suficiente e, obviamente, recursos tecnológicos para proteger as empresas. Este é o cenário que acontece, neste momento, em Portugal. Que não evita que as grandes corporações, mais preparadas, sejam atacadas na mesma, mas isso vai acontecer sempre.

Q4: Mas a verdade é que as empresas, hoje em dia, estão muito mais preparadas do que há uns anos, certo?

RD: Sim, isso é verdade. Houve uma evolução bastante positiva, mas naquilo que é o segundo pelotão – o pelotão das empresas mais pequenas – eu não posso dizer que, neste momento, estejamos numa situação que seja minimamente satisfatória. Ainda há um longo caminho a percorrer nessas empresas.

Q5: Acredita que a formação dos colaboradores poderá ajudar as empresas a melhor prepararem-se em matéria de cibersegurança?

RD: Isso é essencial. Eu costumo dizer muitas vezes que cibersegurança são três vetores: as pessoas, os processos e a tecnologia – eu normalmente trabalho mais na área da tecnologia. E está provado que, se nós trabalharmos nos dois outros vetores, que são as pessoas e os processos, automaticamente teremos de viver menos da necessidade da tecnologia. Eu não concordo muito, às vezes, com a questão da formação. Aquilo que eu acho que é necessário é educação. Educação e formação são coisas completamente diferentes. Eu faço muitas vezes um paralelismo, por exemplo, com aqueles anúncios relativos a "passar na passadeira", "usar o cinto de segurança" ou "se conduzir, não beba". Se reparar, estas campanhas são feitas ao longo de anos e de forma permanente, para que nos eduque e não para que nos forme. Muitas vezes aquilo que eu vejo – mesmo na área da tecnologia – é que nós temos uma formação e se, no imediato, não colocarmos em prática, esbate-se tudo aquilo que nós aprendemos. Porque era uma formação… tem um espaço temporal, às vezes, muito curto. Quando fazemos ações de educação, que são permanentes e visam moldar a pessoa, aí os resultados são significativos. Portanto, aquilo que eu diria é que essas ações

são extremamente importantes. Não só as ações de formação, mas inclusivamente algumas empresas que já compram produtos ou ferramentas que, com regularidade, testam e põem à prova os seus colaboradores, mostrando-lhes que estão errados nas ações que praticam, e isso obviamente faz aumentar significativamente a segurança. Existe aquele clichê de que a pessoa é o elo mais fraco, mas efetivamente continua a ser. Porque se a pessoa não clicar naquele *link*, se não for àquele *site*, se não usar o recurso da empresa de forma indevida, vamos testar menos a *firewall* ou o antivírus. Vai existir menos testes e diminui claramente a probabilidade de uma empresa ser atacada. Portanto, é essencial fazermos essas formações e essas ações, mas eu diria que deveríamos ir mais além, que é educar os colaboradores com ações permanentes.

Q6: Desde 2020, temos vindo a assistir a uma evolução significativa do número de ciberataques a ocorrer em empresas portuguesas. Quais considera ser os motivos que levaram a este aumento nos últimos anos?

RD: O primeiro, obviamente, é a globalização. Nós estamos interligados num mundo global, como todas as empresas, e estamos tão expostos como qualquer outra empresa a nível mundial. O segundo motivo é que apareceram grupos cibercriminosos que começaram a atuar ou a interessar-se pelo mercado português também. Antes de 2020, os ataques de *phishing* que eram feitos em Portugal eram de muito má qualidade, vamos chamar-lhe assim, eram utilizados tradutores automáticos… Hoje, vemos ataques de *phishing* de grande qualidade, com um português correto, que sabem os procedimentos das empresas… Portanto, isto mostra que temos grupos cibercriminosos a atuar especificamente ou para o mercado português ou para o mercado de língua portuguesa. O terceiro motivo tem que ver com o facto do próprio cibercrime ter vindo a evoluir. Tem aumentado o número de cibercriminosos e, obviamente, vindo para um mercado menos explorado como Portugal, podem ter mais sucesso do que estar num mercado a competir entre eles… num mercado francês, num mercado espanhol ou num mercado norte-americano, onde já muitos grupos operam. Nesta questão do cibercrime, há muitas vezes uma tentação de olharmos para isto como uma questão tecnológica. Mas isto é crime puro. O veículo do crime é que é tecnológico. É isto que temos de perceber. Ao longo dos anos, fomos vendo que havia movimentações de grupos que trabalhavam na área das armas ou mesmo do tráfico humano, que passaram a investir na área do cibercrime, porque era mais seguro, existindo menos probabilidade de serem apanhados, e se calhar conseguirem maior proveito. Portanto, o mundo evoluiu, estamos todos interligados e isto obviamente aumentou, sobretudo porque há uma oportunidade de negócio. Basta ver que quando foi a pandemia e nós tínhamos de ter o certificado de covid, apareceram logo *sites* em português a vender o certificado português. Apareceu uma oportunidade de negócio, automaticamente apareceu alguém a tirar partido disso.

Q7: Falou-me da pandemia e gostaria de tocar precisamente nesse ponto. Coincidentemente ou não, o número de ciberataques em Portugal tem vindo a crescer significativamente desde o início da pandemia. Gostaria de saber se o Rui considera que a pandemia também foi um fator que impulsionou este aumento, visto que passámos a estar mais expostos às tecnologias e a adotar o teletrabalho.

RD: Está relacionado com a pandemia, mas eu não diria que é propriamente a pandemia a causa. Está a acontecer no mundo a transformação digital, que começou muito, entre outros fatores, principalmente com a movimentação para a *cloud* e a evolução daquilo que é o Protocolo de *Internet*, que permite mais interligações, mais interações… Permite, por exemplo, que eu tenha um *site* de negócio, que não tem rigorosamente nada, porque tudo são microserviços que o meu *site* lê de outras instituições. Ou seja, o módulo de pagamento é de uma empresa, o módulo de logística é de outra, o módulo de apresentação e a base de dados das fotos é de outra… O *site* é meu, mas nada do que está no meu *site* está em minha posse e é tudo interligado. Deu-se aquilo que chamamos a transformação digital. E é aqui que entra a pandemia, que traz a aceleração da transformação digital. Aquilo que se esperava que acontecesse em 5 ou 10 anos, aconteceu em 2. Ou seja, houve uma evolução gigante daquilo que estava a acontecer. E é aqui que entra, mais uma vez, a oportunidade de negócio do cibercrime. Porque, normalmente, tudo o que é feito a correr não é tão pensado, não se tem tanto cuidado e, principalmente, não se leva em consideração com a segurança. O que as empresas pensaram foi: "vamos para a *cloud*, pomos ali os *sites*, as aplicações, as bases de dados… os utilizadores vão todos para casa e depois logo se vê como é que se fazem as VPN's ou como é que se faz a autenticação". Por isso, a pandemia acaba por ser uma coincidência, porque a pandemia trouxe esta oportunidade para o cibercrime. Como houve uma aceleração desta transformação digital, todos os processos foram feitos muito mais rápido, com menos cuidado e, automaticamente, isto criou um conjunto enorme de oportunidades para os cibercriminosos. Outra coisa que aconteceu – e que está relacionada – é o facto de que, antigamente, o meu portátil estava dentro de um edifício, atrás de uma *firewall* e era mais simples de o proteger. Com a pandemia, fomos todos para casa e aqui a questão é: onde é que está a *firewall* que estava dentro do edifício e que protege agora o portátil que está em casa? Quando se fala de cibercrime, há duas coisas que normalmente nós falamos muito, que estão diretamente relacionadas. Uma é as superfícies de ataque, ou seja, aquilo que eu posso atacar. Antigamente, quando se falava de cibersegurança, tínhamos os PC's todos dentro de um edifício, todos atrás de uma *firewall*, portanto aquele acesso à *Internet* era mais fácil de o proteger. Os vetores de ataque também eram menores… cinco, seis, sete, talvez dez. Quando se dá esta aceleração da transformação digital e nós vamos todos para casa, todos para a *cloud*, aquilo que nós chamamos

de superfícies de ataque são enormes. É e continua a ser o edifício onde eu estava, é a casa de cada uma das pessoas da minha empresa, temos os dispositivos móveis que agora se ligam e também têm os mesmos dados que o computador, temos a *cloud*, temos a interligação com todos os fornecedores… Ou seja, aquilo que são as superfícies que eu posso usar para atacar uma empresa são gigantes. Por exemplo, se eu tinha uma superfície de ataque com cinco vetores. Se agora eu tiver dez superfícies de ataque com cinco vetores, eu passei para dez vezes mais a possibilidade de ser atacado. É por isso que, durante a pandemia, para o cibercrime isto tornou-se um mundo maravilhoso.

Q8: Qual é o atual panorama de ciberataques em Portugal? Ou seja, os tipos de ataque mais frequentes, os setores de atividade mais vulneráveis e os riscos inerentes mais verificados nas empresas.

RD: Um dos ataques mais comuns que nós vemos hoje é o *phishing*. O *phishing* está no topo. O *phishing* não é, *per si*, o ataque. O *phishing* é um veículo para o ataque, porque aquilo que se obtém do *phishing* normalmente são credenciais. Normalmente, os atacantes o que fazem é pegar nessas credenciais, tentam depois correlacioná-las com empresas, com recursos ou com sistemas, e depois é que se dá outro tipo de ataques, como acessos indevidos, personificação, utilização de contas, coisas deste género. Mas o *phishing* continua no topo. A seguir temos o *ransomware*, que continua a ser claramente um problema. O r*ansomware*, no passado, era algo que encriptava e pedia dinheiro. Neste momento, já vamos na situação do *triple ransom*. Temos de olhar para os cibercriminosos sempre desta forma: os cibercriminosos querem dinheiro ou querem um benefício qualquer. Portanto, não é uma questão tecnológica. Os ataques podem ser tecnológicos, como roubar um *username* ou uma *password*, tirar uma vulnerabilidade de um sistema e entrar nesse sistema, ou pode ser um recurso extremamente simples, como fazer uma chamada e ganhar acesso a um computador. São vários os tipos de ataque, porque o que interessa é ter aquele proveito. Depois temos outros *malwares* que correm nas redes. Continuamos a ter muito o *brand phishing* ou *backdoors*. As áreas que vemos serem mais atacadas são a área da educação, da saúde e também da administração pública. Às vezes, temos de perceber que os interesses podem não estar diretamente relacionados com valor, ou seja, o valor é relativo. Obviamente se eu vou a um banco, aquilo que eu quero roubar é dinheiro. Mas se eu vou a outra empresa que não tem dinheiro, ela terá outro valor para mim. Poderá ter *usernames* e *passwords*, poderá ter bases de dados, poderá ter moradas… Portanto, o valor é relativo. Como, muitas vezes, as áreas que são atacadas também são relativas. Por exemplo, porque é que há tanto *phishing*? Obviamente que há *phishing* porque há interesse, para, depois de se obter as credenciais, se poder fazer outro tipo de ataques. Por exemplo, porque é que a área da educação, às vezes, é tão atacada? Porque se for um ambiente

mais aberto, mais descontraído, eu posso conseguir um grande número de agentes infetados para, posteriormente, fazer os ataques. Não sei se já ouviu falar das *botnets*. As *botnets* são milhares de máquinas que estão infetadas e os seus utilizadores não sabem que elas estão infetadas. Elas podem fazer várias coisas: podem fazer mineração de criptomoeda, ou seja, para eu não ter de comprar servidores ou ter *data centers* para minerar; podem fazer *spam*, porque o *spam* normalmente tem 0,001 de sucesso, portanto eu preciso de gerar mesmo muitos *e-mails* para ter sucesso comercial com o *spam* – se as pessoas montarem um servidor e meterem num *data center*, ficam automaticamente numa *blacklist* de *spam*, mas se tiverem milhares de agentes espalhados a fazer *spam* por eles nunca ficam na *blacklist* e têm mais sucesso; podem ser utilizados como agentes para fazer ataques de *denial-of-service*, para depois dentro de uma rede propagar o *malware*.

Q9: E relativamente aos riscos mais verificados nas empresas portuguesas?

RD: Já tem acontecido – não com muita frequência, mas tem acontecido – existirem empresas que acabaram por fechar com ataques de *ransomware* sérios, não tendo capacidade de recuperar. Eu há pouco perdi-me e era isso que ia dizer. O *ransomware* evoluiu muito. Numa primeira fase, era encriptar e alguém pagar. Numa segunda fase, eles primeiro retiram dados da empresa e dizem à pessoa "ou pagas ou nós vendemos os teus dados" – chamávamos a isto o *double ransom*. Agora estamos numa fase do *triple ransom*, em que eles fazem isto e, em simultâneo, vendem mesmo os dados na *dark net*. Começámos a ver que o *ransomware* também serve, muitas vezes, para mascarar outro tipo de ataques, o que é ainda mais perigoso. Ou seja, são utilizadas as ferramentas de *ransomware*, que têm várias componentes: a infeção, a propagação na rede e a encriptação. Só para ver a complexidade destes *malwares*. E eles quando fazem isto, fazem isto para maximizar o proveito, para pressionar as empresas a pagar. E continuam a ter muito sucesso. Porque é que a área da saúde começa aqui a aparecer como área de ataque? Porque se a área da saúde tiver um ataque de *ransomware*, a probabilidade de pagar é muito grande, porque estão vidas em risco. Estar ali a negociar ou tentar repor um *backup* é muito complicado, mas é o caminho que se deve fazer. Não se deve pagar, porque pagar é dizer a quem ataca que vale a pena continuar a atacar.

Q10: Toda a nossa conversa tem girado em torna da importância da cibersegurança. Mas eu gostaria que o Rui me dissesse qual é realmente a importância de uma organização segura, ou seja, o que assegura e o que previne, interna e externamente.

RD: A importância é vital. Não sei se conseguiria utilizar um termo mais certo. Se calhar há 5 anos, a cibersegurança não aparecia nas top 10 prioridades. Se calhar há 6/7 anos, aparecia em sétimo ou oitavo lugar. Nos últimos anos, aparece em terceiro lugar. Isto segundo o Fórum Económico Mundial. Portanto, está no topo das preocupações mundiais. E é muito simples. Nós

estamos a desmaterializar, estamos a viver num mundo cada vez mais interligado e dependente da *Internet* e dos sistemas informáticos. Até mesmo sistemas muito básicos, como a água e a eletricidade, dependem de um sistema informático que faz a gestão. Nós nem damos conta, julgamos que é apenas água a correr nos tubos e chega à torneira das nossas casas. Pelo caminho há centenas de sistemas eletrónicos que gerem, remotamente, as estações elevatórias, bombas de água, que abrem comportas, fecham comportas… Se alguém fizer um ataque a um sistema destes, automaticamente podemos não ter água numa cidade durante umas horas muito grandes. Uma empresa pode perder completamente o seu negócio… E isto aconteceu há uns anos quando a maior empresa de logística do mundo tinha todos os seus barcos, aviões e camiões, mas não conseguia transportar um único contentor que fosse. Isto porquê? Teve um ataque de *ransomware* que encriptou todos os sistemas e toda aquela panóplia de mecanismos físicos só funcionava se houvesse um sistema informático a funcionar. Hoje o dinheiro é cada vez menos físico. Mesmo para nós acedermos ao dinheiro físico, precisamos de sistemas informáticos. Basta ver que, muitas vezes, muitos dos salvamentos que se fazem em muitos bancos são para evitar o colapso dos sistemas. Não é para evitar que aquele banco caia, é para que haja o efeito de contágio a outros bancos e que, então, haja o caos num país ou região, porque um banco faliu. Agora imagine se não houver dinheiro nas caixas multibanco… é o caos completo. Eu poderia estar aqui a dizer-lhe muito mais exemplos da gravidade que um ataque a sério a um sistema pode provocar e da importância que a cibersegurança tem. Portanto, eu diria que ela é vital para a vida como nós a conhecemos hoje. Contudo, continuo a achar que ainda não é dada a importância devida a este tema. Ainda não há orçamentos necessários, ainda não temos recursos humanos necessários e suficientes e especialistas para promover estas áreas… Continuam-se a desenvolver aplicações e sistemas, em que primeiro se desenvolve a aplicação e só depois é que se pensa na cibersegurança. Não é feito o *security by design*, ou seja, a aplicação não é feita com a segurança já interligada. Por isso, é essencial a cibersegurança para um mundo como o conhecemos hoje.

Q11: Relativamente a medidas de segurança, quais considera ser as medidas necessárias a implementar por uma organização em situação de ciberataque?

RD: Em primeiro lugar, deve-se educar as pessoas. Educando as pessoas, automaticamente reduzimos o risco, se calhar de uma forma drástica. Não clicando num determinado *link*, não colocamos os sistemas à prova. Porque não há sistemas infalíveis… E porquê que há vulnerabilidades? Há uma vulnerabilidade porque há pessoas a desenvolver código, que não é corretamente desenvolvido. Por isso, é muito importante que as pessoas colaborem e participem na segurança, não colando à prova os sistemas de cibersegurança. Outro aspeto: é essencial os processos. Quando falamos de processos, falamos do ISO 27001, ou no PCI, ou no SOX… todos

aqueles *compliences* enormes que existem e que são aplicados, normalmente, à área das *utilities*, à área da água ou da luz, à área da banca ou à área da saúde. Mas há outras normas mais simples, que podem e que devem ser aplicadas e que automaticamente aumentam a segurança. Entre elas, por exemplo, definir o que é informação crítica, confidencial ou pública. Só por isto, automaticamente obriga-me a ter uma forma diferente de ver a informação e decidir quem é que acede a esta informação. E ao fazer uma coisa tão simples como isto, eu vou criar controlos de maneira que, quem não tem autorização, não tem acesso à informação. E automaticamente, com isto, estou a dificultar a vida também a quem ataca. Porque se eu não tenho estes controlos e uma das pessoas mais vulneráveis é atacada, automaticamente eles chegam à informação. Por incrível que pareça, é uma coisa tão simples que qualquer empresa podia fazer e aumentava brutalmente a segurança nas empresas. Portanto, é fundamental ter processos muito claros. Há uma outra coisa que é essencial para as empresas fazerem – e que começamos agora a falar mais – que é "Fui atacado! E agora?". Isto é essencial para as empresas. Andamos todos muito focados – apesar de eu achar que não o suficiente – em nos proteger, mas temos de estar tão focados na resolução do problema e ter um procedimento de resposta ao ataque. Às vezes, quando as empresas são atacadas, começa-se a desligar tudo, anda tudo a correr de um lado para o outro, não se sabe comunicar, nega-se o acesso aos dados, não se sabe onde estão os *backups*… Portanto, é importante as empresas começarem a pensar desta forma: "fui atacado, está tudo encriptado, agora então o que é que eu vou fazer?". Então ter um procedimento de resposta ao ataque, que permite ter calma, fazer as coisas de forma correta e permite que as empresas recuperem como deve ser. Outra coisa que é importante as empresas fazerem é ter um plano de recuperação. Não é só um plano de recuperação do próprio ataque, mas um plano de recuperação do negócio. Assumir que a parte tecnológica é essencial para a sua sobrevivência e, por exemplo, terem aquilo que no passado existia e que agora se deixou de fazer e, por isso, é que temos tido tantos problemas, que é *backups* chamados *offline*. Ou seja, ter *backups* que não estão ligados em lado nenhum. Antigamente, eu fazia *backups* de megas, 200 megas, 500 megas, 1 tera, no máximo. Agora, tenho de fazer *backups* de 10 teras, 20 teras, e já começamos a falar em *petabyte* e outras coisas. Portanto, é impossível fazer *backups* desta quantidade de informação para sistemas físicos. Então começou-se a fazer *backups* de disco para disco. Temos um sistema de *backup* ali ao lado, com discos ultrarrápidos e com sistemas de compressão. Mas depois o que é que fazemos? O sistema de *backups* está ligado na rede e tem a mesma *password* da rede. O que é que os atacantes fazem? Quando atacam, a primeira coisa que eles fazem é apagar o *backup*. Portanto, as empresas têm de voltar a fazer procedimentos de *backup offline*. Outra coisa que acontece – e também já aconteceu a algumas empresas – é o *backup* não estar no disco ao lado, mas estar na *cloud*. Mas é exatamente a mesma coisa, porque as ligações hoje para a *cloud* é como se fosse para o disco, para um servidor que está

ali num *data center* ao lado. E utiliza-se a mesma *password*, porquê? Não há um processo que defina que as *passwords* são diferentes e, então, o pessoal do IT, para ser mais fácil fazer a sua gestão do dia-a-dia, utilizam a mesma *password* para não ter trabalho. Quando os atacantes fazem um ataque de *phishing* e apanham a *password*, a *password* serve para tudo. Portanto, é essencial isto fazer parte do plano de recuperação de um ataque que as empresas devem ter. Por último, obviamente as empresas devem investir em cibersegurança. Falta-me aqui os próprios recursos humanos, eu falei na formação dos utilizadores, mas falta-me também os recursos da própria empresa. Eles têm de ter *know-how*, eu não posso converter pessoas de aplicações ou de bases de dados para pessoas de cibersegurança. Devem, sim, ter pessoas com formação adequada nesta área. E, por último, obviamente, ter tecnologia adequada e não se comprar a falsa sensação de segurança. O antivírus *free* não é *free* e não é seguro. E um fabricante que é muito barato versus a média dos fabricantes que são considerados de topo não é uma solução segura, de certeza deve ter algum *handicap*. E isto tem de ser levado em conta.

Q12: Há pouco falou-me da importância da comunicação. Considera a comunicação fundamental nestas situações?

RD: Eu acho que é, sem dúvida, essencial. Eu tenho visto os ataques que se têm dado e, às vezes, a comunicação não é feita da melhor forma. Acho que o melhor exemplo que nós temos é o da Vodafone. Eles, de imediato, assumiram o ataque, fizeram um plano de comunicação permanente. Para já, porque é um sistema extremamente crítico para o país e para os clientes que têm… E acho que isso teve um efeito positivo e não negativo. Porque, muitas vezes, tenta-se esconder os ataques, tenta-se esconder a real profundidade do ataque, para tentar, de alguma forma, não denegrir muito a imagem da empresa. Mas depois isto tem um efeito perverso e negativo, que é, quando mais tarde se percebe que afinal os sistemas não eram assim tão bons e que os dados foram expostos, as coisas tornam-se mais negativas e, então, há uma perceção de desconfiança. Comparando outros ataques que não foram claros os motivos da comunicação versus aquilo que foi feito no caso da Vodafone, eu vejo, por exemplo, que nos sentimos todos se calhar mais seguros, porque eles assumiram o ataque e foram claros na sua comunicação. Principalmente quando é uma empresa que presta este tipo de serviços e que tem outros a depender desses serviços, uma comunicação que seja assertiva e clara também tira pressão de cima das próprias equipas que estão a trabalhar, porque dá-lhes mais paz de espírito para desenvolver o trabalho. Vamos supor que a Vodafone, em vez de assumir que estava a ser atacada, utilizava um discurso pouco claro sobre o ataque. Os clientes iriam, seguramente, continuar a ligar vezes sem conta a dizer que queriam o serviço, queriam a *firewall*, queriam o servidor, queriam o dispositivo móvel. Porquê? Porque não estava claro o que tinha acontecido. Tendo eles assumido claramente, desde a primeira hora, o ataque e

tendo mantido um plano de comunicação do estado da situação daquilo que estava a ser feito e daquilo que estava a ser recuperado, eu, que sou cliente e que recebo a informação, não tenho tanta necessidade de ir obter essa informação. São estes os aspetos que eu considero mais relevantes entre o tentar esconder o ataque ou as reais dimensões do ataque e ter uma comunicação mais clara. Eu acho que é claro entre todos que os ataques podem acontecer a qualquer um, portanto acho que já é altura de deixarmos de tentar esconder que sofremos um ataque e que os dados foram expostos.

Q13: Quais considera ser as principais tendências e desafios na área da cibersegurança? Já me falou da *cloud* e da globalização, mas quer acrescentar mais alguma?

RD: A globalização e a *cloud* continuam, inevitavelmente, a ser um desafio muito grande. Porque a *cloud* é algo muito novo, que está a evoluir a uma velocidade muito grande e, às vezes, não há recursos suficientes para acompanhar essa evolução. Por exemplo, há recursos de quem desenvolve a *cloud*, mas não há recursos depois de quem é cliente e vive da própria *cloud*. E isso vai continuar a gerar desafios. O facto de estarmos a migrar tudo para a *cloud* e a velocidade com que temos de gerar novas aplicações, novos conectores, novas funcionalidades, também é um desafio muito grande. Só para ter uma ideia, nós já temos soluções que pretendem entrar dentro do ciclo de desenvolvimento da *cloud*, uma vez que é extremamente rápido e uma das coisas que faz é desenvolver as coisas em produção. Antigamente, eu desenvolvia uma aplicação no meu computador e, mais tarde, eu colocava-a em produção. Na *cloud*, muitas vezes, eu estou a desenvolver a aplicação em produção. Em termos de cibersegurança, isto pode ser muito grave, porque se eu desenvolver mal e tiver uma vulnerabilidade, automaticamente posso dar acesso à minha aplicação. Quando tivermos o 5G efetivamente em todo o seu potencial, então vamos ter aí também um grande desafio, porque é quando tudo se interligar com tudo e, muito provavelmente, deixarmos de usar as redes tradicionais. Ou seja, a rede móvel e a rede do escritório é tudo o mesmo e tudo se interliga. Isto vai fazer com que apareçam uma série de dispositivos que, provavelmente, até hoje estavam escondidos, como câmaras, como sensores, como portões, como lâmpadas… aqueles dispositivos do IoT que estão todos interligados e que vão aumentar brutalmente as tais superfícies de ataque e, consequentemente, os vetores de ataque. Esta é outra preocupação que vai acontecer no futuro. Estas novas redes trazem, lá está, um novo paradigma da segurança. Eu neste momento estou habituado a colocar uma *firewall* e, atrás da *firewall*, coloco tudo o que eu quero proteger. Quando tudo estiver interligado, eu coloco a *firewall* onde? Portanto, isto cria um novo desafio da própria abordagem da cibersegurança no mercado. E quando chegar o 6G, com mais interligação e com mais dispositivos, então ainda maiores vão ser os desafios que vamos ter.

Q14: Por último, gostaria de saber qual considera ser o futuro dos ciberataques.

RD: Obviamente, o que vamos assistir é a um aumento significativo dos ciberataques. Principalmente, enquanto não conseguirmos ter uma evolução clara da cibersegurança. Há aqui duas questões na cibersegurança: primeiro, é se tecnologicamente há evolução ou não e isso é um desafio; segundo, é as empresas assumirem que têm de investir e que têm de levar este tema a sério. Vamos supor que já temos um *gap* tecnológico e, se juntarmos um *gap* de falta de recursos e de falta de meios financeiros, então o *gap* será gigante. Temos de tentar chegar a uma fase em que o único *gap* que temos é o *gap* tecnológico. Portanto, eu não lhe sei dar uma resposta quanto ao futuro dos ciberataques. É uma pergunta que me fazem muitas vezes e, uma vez, perguntei a um dos meus VP's da área de desenvolvimento e o que ele me respondeu foi: "Rui, o futuro dos ciberataques é onde estiver uma oportunidade". Portanto, é muito difícil prever. Nós só conseguimos fazer previsões a breve trecho. Se calhar, antes do covid, ninguém iria dizer que o covid viria trazer uma panóplia gigante de oportunidades para os ciberatacantes. Os *sites* de rastreio do covid foram utilizados para ataques, os *sites* dos certificados de covid foram utilizados para ataques, os *sites* das vacinas foram utilizados para ataques… A guerra na Ucrânia está a ser usada massivamente para ataques, quer para disseminar armas de ataque a supostos exércitos que devem ajudar a Ucrânia, mas depois essas armas vão estar a navegar livremente sabe-se lá na mão de quem, quer *sites* que pedem dinheiro para a Ucrânia e são falsos. Portanto, depende muito do que acontecer nos próximos tempos no mundo. Obviamente, há aqui uma tendência: a *cloud*, o IoT e o 5G. Aqui nós vemos uma tendência e devemo-nos preocupar. Tudo o resto é muito difícil de prever. Há uma pergunta que não me fez e eu acho que é muito importante, que é: quem são os atacantes? Nós temos diferentes tipos de atacantes. Temos aquilo que nós chamamos os *state-sponsored attacks* e que são altamente perigosos. Têm duas vertentes: uma vertente bélica, que é deitar sistemas inimigos abaixo; e outra vertente de deitar sistemas críticos abaixo, como água, luz, bancos, *Internet*, televisão… Depois temos aqueles que querem só fazer umas brincadeiras. Depois temos os *hacktivistas*, pessoas que têm ideologias contra determinado tema ou área. E, por último, temos o cibercrime, que se parte numa panóplia gigante de pessoas que querem valor. Uns querem valor sobre a forma de dinheiro, outros querem valor sobre a forma de informação que, mais tarde, vão vender. Cá está, para se falar no futuro, temos de olhar para todos estes atores dos ciberataques e perceber que oportunidades novas cada um deles vai ter. Por exemplo, a *cloud* pode ser utilizada por uma nação para atacar outra. Porque não? Se todos os sistemas desse país tiverem na *cloud* e serem geridos a partir da *cloud*, se eu desligar a *cloud* a esse país, todos os sistemas são desligados. Vamos supor um caso extremo. As nossas empresas de serviços começam todas a meter na *cloud* os sistemas de gestão que são essenciais para que tudo funcione e esses sistemas

de gestão são feitos por um prestador de serviços que não é nacional – e os principais prestadores de serviço de *cloud* não são nacionais. Vamos supor que um dia, por algum motivo, nos chateamos com o país onde está esse prestador de serviço. O que é que impede esse país de cortar o acesso à *cloud* dos nossos sistemas? Nada. Portanto, está aqui uma oportunidade de um país, no futuro, fazer um ciberataque a outro país. É tão simples quanto isto. O futuro é muito difícil de prever, mas vamos continuar a ver o *ransomware*, o *phishing*, vamos começar a ver a Inteligência Artificial cada vez mais nos ciberataques – e isso é uma preocupação –, vamos começar a ver computação quântica, quando ela for desenvolvida a sério e envolvida nos ciberataques – também é uma preocupação. Neste caso, as nossas VPN's passam todas a estar vulneráveis, porque um computador quântico passará a conseguir desencriptar facilmente aquilo que é o nosso tráfico encriptado. Isto é uma previsão, tudo o resto depende do que vai acontecer no mundo.

Apêndice 3: Entrevista Mauro Almeida

Q1: Gostaria que o Mauro começasse por me falar um pouco sobre a sua experiência na área da Cibersegurança.

Mauro Almeida (MA): Tirei a minha licenciatura em Engenharia e Sistemas Informáticos. Fiz grande parte da minha vida profissional pelo percurso de desenvolvimento de *software*. Sempre tive muito ligado a uma componente tecnológica e de arquiteturas. E depois quis fazer a transição mais pela componente de gestão. Sensivelmente em 2012, fui trabalhar para uma empresa que está mais centrada na componente de certificados digitais, *public infrastructures*, assinaturas eletrónicas, componente de criptografia aplicada… Portanto, foi aí que eu comecei a trabalhar um bocado mais ativamente a componente toda de segurança. Tive muito ligado a projetos relacionados o cartão de cidadão, chave móvel digital, passaporte eletrónico, etc. Portanto, sempre numa componente de solução tecnológica, mas também obviamente que toca nos temas das políticas, procedimentos, principais normativos… Depois, em 2017, tomei a decisão de investir novamente na minha formação e fui fazer um MBA. Senti que seria a formação que iria complementar um pouco o que é o meu *background* tecnológico e a minha experiência profissional, com uma visão mais económica, financeira, comercial, gestão de empresas, política de empresas… Terminei em 2019, altura em que surgiu também a oportunidade numa empresa anterior, em que estava responsável pelo departamento de projetos, sendo que a empresa tinha uma orientação mais para a componente de produto, toda a componente de desmaterialização *onboarding* de clientes, componente de autenticação, autorização, assinaturas eletrónicas, sempre muito ligado também à componente de certificados digitais, como tinha dito. Portanto, no final de 2019 surgiu a oportunidade de integrar a empresa onde estou atualmente como Diretor de

Cibersegurança. Sou responsável de uma unidade de negócio. Tem uma oferta diversificada, desde uma componente mais estratégica, *de governance, risk and compliance*, uma componente de *awareness*, sensibilização, principais normativos, regulamentos, até à implementação de soluções, sejam baseadas em soluções de segurança e *compliance Microsoft* ou também para a componente de gestão e governo de identidades, gestão e controlo de acessos, com outros parceiros e outras soluções tecnológicas.

Q2: Qual é a sua opinião relativamente à evolução dos ciberataques em Portugal?

MA: Quando se fala de ciberataques e de cibersegurança, não há fronteiras. Portanto, Portugal tem seguido um bocado a tendência internacional. Vou-te dizer aqui duas vertentes. Uma é a complexidade e a criatividade dos ataques, ou seja, eles têm-se tornado cada vez mais complexos de se defender, de detetar e de mitigar, também pela panóplia de ferramentas, de soluções tecnológicas e da própria evolução tecnológica, que está não só à disposição de quem está a defender as organizações, como também de quem as está a atacar. Portanto, todas estas evoluções tecnológicas – desde o 5G, Inteligência Artificial, computação quântica, que ainda está a dar os primeiros passos, mas que já é uma preocupação muito grande a nível governamental e a nível das empresas –, numa perspetiva tecnológica têm acompanhado a evolução das outras tecnologias emergentes. Por outro lado, numa perspetiva de tendências, Portugal tem também acompanhado a tendência internacional, ou seja, um aumento do número de ciberataques e eu diria, na minha opinião, essencialmente por dois motivos. Primeiro, pela quase democratização de acesso a ferramentas e serviços de ciberataques, ou seja, hoje em dia já é possível adquirir *toolkits* de forma gratuita ou a muito baixo custo para perpetuar determinados tipos de ataques. Depois começa-se a assistir também a uma concentração grande de grupos profissionalizados, que fazem este tipo de ataques, seja numa ótica de serviço, ou seja, tu contratares o serviço para fazer determinado ataque, seja numa ótica de ganharem notoriedade e relevância dentro do meio ou para fins financeiros e económicos, e até numa ótica de ativismo. Portanto, eu diria que isto é a tendência natural. Depois acho que existem naturalmente alguns picos, ou seja, normalmente os atacantes tiram partido de situações de pressão nas sociedades ou nos indivíduos, tiram partido do sentido de urgência e do próprio receio e, portanto, é comum que algumas situações, como foi, por exemplo, a crise económica de 2008, de 2012, a crise que passámos agora com a pandemia, toda a situação de aumento da inflação e obviamente a guerra entre a Rússia e a Ucrânia, acabem por acentuar um pouco aquilo que são estes tipos de ataques. Por exemplo, assistiu-se a um aumento muito grande da aquisição de domínios relacionados com covid, que depois foram utilizados por atacantes para ações de *phishing*, criação de *malware* nos dispositivos, etc. Portanto, há estes picos que são naturalmente uma forma mais ou menos explorada pelos atacantes.

Q3: Desde 2020, sensivelmente, temos vindo a assistir a um aumento significativo do número de ciberataques. Quais considera ser os principais fatores que impulsionaram este aumento?

MA: Centrando um bocado no tema pandémico, ao contrário da crise de 2008, a pandemia teve um efeito curioso. Primeiro, foi uma crise progressiva, ao contrário da de 2008, ou seja, foi havendo um contágio progressivo e cada país tinha depois os seus mecanismos macroeconómicos para dar resposta a isso. A pandemia foi quase imediata e, de um momento para o outro, as empresas tiveram duas grandes preocupações. A primeira foi garantir os seus compromissos financeiros com os colaboradores e com os parceiros, ou seja, pagamento de ordenados, pagamento aos fornecedores, garantir liquidez, porque houve uma incerteza muito grande também relativamente ao negócio. Portanto, houve um desinvestimento imediato ou redireccionamento daquilo que eram os orçamentos que eventualmente já estariam previstos para o tema da cibersegurança, o que expõe logo mais as organizações. Depois o nível de maturidade em cibersegurança das organizações em Portugal também não estava num estado ótimo. Já havia – e continua a haver muito – essa sensibilização. Há um trabalho muito bom que tem sido feito por parte do Centro Nacional de Cibersegurança de sensibilização e apoio às empresas. E estou até a desconsiderar aquilo que é o tecido empresarial de pequenas e médias empresas, que estão mais expostas e que têm menos capacidade de investimento. Mas, portanto, havia uma sensibilização e um sentido de que as empresas deveriam investir na cibersegurança. Há uma discrepância entre algumas empresas naquilo que é o nível de maturidade, mas, de uma forma geral, não estavam num elevado nível de maturidade. Depois, de um momento para o outro, as empresas viram-se obrigadas a estender a sua área de atuação literalmente até à casa do colaborador. Portanto, as pessoas estavam numa rede doméstica, não estavam numa rede corporativa, com menos controlos de segurança implementados, numa rede que não era controlada corporativamente, muitas vezes com dispositivos pessoais a serem utilizados para aceder a ativos da organização. Quando não eram dispositivos pessoais, muitas das vezes os dispositivos corporativos eram utilizados também por outros membros do agregado familiar para temas pessoais ou até pelo próprio colaborador. Portanto, todo este perímetro de segurança que existia ou que estava mais ou menos delimitado àquilo que era a infraestrutura da organização deixou de existir ou estendeu-se até à casa do colaborador. Naturalmente, isto expôs as organizações a outros vetores de ataque.

Q4: Portanto, considera que a pandemia foi o principal fator ou acrescentaria mais algum?

MA: Não acho que tenha sido o principal. Acho que, de todos, este foi aquele que mais expôs as organizações. Mas o incremento dos ataques tem vários fatores associados. Desde a democratização do acesso a algumas ferramentas de *hacking*… Houve aqui vários contributos para isso, alguns dos quais já fui mencionando.

Q5: Também me falou sobre o grau de maturidade das empresas. Qual considera ser atualmente o grau de preparação das empresas portuguesas em cibersegurança?

MA: Isso é uma pergunta muito difícil. Não lhe consigo quantificar, mas posso dar-lhe uma opinião. Tem havido um grau de maturidade que está a crescer consideravelmente. A cibersegurança já é um tópico discutido a nível dos conselhos de administração, já existe essa sensibilização. O risco cibernético já é considerado em muitas organizações e tratado como um risco operacional. Portanto, esse nível de consciencialização e de sensibilização tem aumentado bastante, o que é muito positivo. Os ataques que temos assistido em Portugal, nomeadamente no início de 2020 e ao longo dos últimos anos, tem sensibilizado cada vez mais as organizações para isto. Numa perspetiva de implementação, acho que algumas organizações ainda têm dificuldade em perceber como é que devem fazer o seu investimento em cibersegurança e por onde é que devem evoluir. Isto porque o mercado em cibersegurança tornou-se muito apetecível nos últimos anos, para quem faz essa venda de serviços, produtos, soluções… E, portanto, como esta oferta começa a ser tão grande, às vezes as organizações sentem-se um bocado exacerbadas, no sentido em que têm alguma dificuldade em perceber o que devem contratar, onde devem contratar, que serviços devem ou não implementar. Eu diria que isto é fundamental. Primeiro, porque os recursos são escassos, seja humanos, financeiros, tecnológicos, etc. E depois porque aquilo que funciona numa determinada organização em termos de cibersegurança não é aquilo que vai funcionar noutra organização que esteja a operar eventualmente no mesmo setor e que tenha a mesma dimensão em termos de colaboradores ou complexidade tecnológica. Porque isto vai estar sempre muito inerente àquilo que é a cultura organizacional, à sua própria apetência para o risco, à sua *landscape* tecnológica… Ou seja, há muitos fatores que vão influenciar aquilo que deve ser um plano estratégico de cibersegurança dentro de uma organização.

Q6: Considera, então, importante as organizações apostarem na formação dos seus colaboradores?

MA: Mais do que importante, eu diria que é fundamental. Isto porque, independentemente do valor que as empresas invistam em soluções tecnológicas e que eventualmente forcem as ações ou os comportamentos dos colaboradores, a pessoa há de ser sempre a primeira linha de ataque ou a primeira linha de defesa, dependendo quão sensibilizada estiver ou não para a cibersegurança. A cibersegurança tende a ser um tema enfadonho para quem está a ouvi-lo numa ótica de sensibilização. Para que as pessoas mudem um bocado os seus comportamentos, é importante que sejamos capazes de mudar as suas convicções e que percebem qual é o impacto desses seus comportamentos, quer para a sociedade, quer para a organização. Portanto, eu diria que é fundamental esta componente de sensibilização. A forma como ela tipicamente é feita não

considero que seja a melhor. Faz parte já das políticas de um grande número de organizações haver esta sensibilização dos colaboradores, mas, muitas das vezes, ela é feita de forma uniforme a toda a organização, sem grande distinção entre o indivíduo e, em algumas situações, até mais difícil ainda, é feita da forma mais simples que é juntar as pessoas numa sala, dar-lhes uma formação e uma sensibilização de segurança. Hoje em dia, com o remoto, até é mais fácil, porque se cobre grande parte da organização. Mas isto tem uma limitação muito grande que é as pessoas não assimilam os conteúdos e não há um *engagement* das pessoas para com esta informação. Portanto, é fundamental ter formas criativas e diferentes de passar esta mensagem aos colaboradores. E conseguir também medir e auferir qual a maior ou menor propensão de uma pessoa para cair em determinado tipo de ataque ou ter determinado comportamento de risco e que vai ser diferente dentro da própria organização entre os seus colaboradores.

Q7: Qual considera ser o atual panorama de ciberataques em Portugal? Ou seja, quais os tipos de ataque mais frequentes, os setores de atividade mais vulneráveis e os principais riscos decorrentes de um ataque verificados nas organizações.

MA: Os tipos de ataques mais frequentes tem sido muito a componente do *ransomware* e do *phishing*. Aliás, não te consigo precisar se esses são os mais frequentes ou não. Saiu agora, inclusivamente, um relatório do Centro Nacional de Cibersegurança para 2022 relativamente a esta componente de cibersegurança e de certeza – ainda não tive oportunidade de o ler – que falam lá quais foram os principais tipos de ataque em território nacional. Se não houver uma grande alteração relativamente ao ano anterior, eu diria os ataques de *phishing* e de *ransomware*. Em termos de setor, eu acho que não faria aqui uma distinção em termos da vulnerabilidade do setor. Faria sim, talvez, do quão apetecível é um determinado setor em detrimento de outro. Portanto, tudo o que são infraestruturas críticas dentro de um país, banca ou instituições financeiras, naturalmente, são mais apetecíveis, porque a quebra de um serviço de uma infraestrutura crítica tem um impacto brutal a nível da sociedade. A banca, naturalmente, é apetecível pelo tipo de negócio que tem, assim como as grandes empresas. Por outro lado, é preciso não descurar as empresas de menor dimensão – e não falo só das PME's, falo também do segmento de *corporate* – porque nós temos de olhar para as empresas como um conceito de ecossistema alargado e, portanto, hoje em dia já não é só uma determinada empresa que tem de estar preocupada com a sua postura de cibersegurança, mas tem de olhar também para aquilo que são os seus fornecedores, porque é uma componente que, muitas vezes, é descurada. Portanto, muitas das vezes estas empresas de menor dimensão são utilizadas como um veículo ou como um vetor de ataque para entrar dentro da empresa que, em última instância, os atacantes querem realmente atacar. Falando agora do impacto, eu acho que vai depender de empresa para empresa. Por exemplo, em termos

estatísticos, acho que 60% ou 70% das PME's que são atacadas fecham portas nos 6 meses seguintes. Isto revela logo a fragilidade e a capacidade de resposta de uma PME àquilo que é o ciberataque. Também porque tipicamente têm menos capacidade de investimento em segurança e daí a importância do associativismo e de criar estas corporações entre PME's que operam no mesmo setor. Depois, dependendo de empresa para empresa, porque cada caso é um caso, o tema reputacional. O dano reputacional é aquele que é mais difícil de quantificar, mas um dos que pode ter mais impacto para a empresa a médio-longo prazo, ou seja, começarem a perder clientes, começarem a perder confiança por parte dos parceiros, por parte do consumidor e, logo aí, assiste-se a um decréscimo naquilo que é o volume de negócio. A maior parte das empresas sabe e é fácil compreender que é muito mais fácil reter um cliente do que adquirir um novo. Se há uma perda de clientes, é um ciclo vicioso que deve ser quebrado. Portanto, este tema da notoriedade é importante. Depois, obviamente, o impacto de quebra operacional. Recordo-me que havia uma empresa, há uns anos, que foi atacada, teve dois ou três dias parada por causa de um ataque de *ransomware* e teve um impacto de cerca de 2 milhões de euros – e falamos, então, do impacto financeiro. E depois eventuais coimas ou multas que possam ser aplicadas por parte dos reguladores, nomeadamente a Comissão Nacional de Proteção de Dados para temas de proteção de informação e dados pessoais.

Q8: Já temos vindo a falar muito sobre isso, mas gostaria de saber qual considera ser a importância de uma organização segura, ou seja, o que assegura e o que previne, tanto a nível interno, como a nível externo.

MA: Para começar, há aqui um conjunto normativo e de regulamentos europeus que estão em marcha, nomeadamente o *Digital Operational Resilience Act* e outros, que já foram aprovados, inclusivamente, e que existem numa ótica de dar ao consumidor que consome serviços e produtos digitais uma maior segurança daquilo que está a comprar. Isto vai obrigar a que as empresas tenham de dar resposta a estes normativos e vai obrigar a que elas também trabalhem internamente para se dotarem das capacidades e dos controlos de segurança necessários para dar esta confiança ao mercado. Portanto, já está a haver uma grande aposta e movimentação numa perspetiva legislativa, a nível europeu, para trazer este conforto para os clientes. Numa perspetiva interna, é fundamental a organização estar segura para evitar disrupção de serviço, para evitar quebras operacionais, para evitar multas, para evitar perda reputacional no mercado em que opera. Isto obviamente tem impactos internos e externos, é difícil dissociar os dois. Se uma determinada empresa é atacada, há uma perda de confiança por parte do mercado, há uma perda de confiança por parte não só dos clientes, mas dos fornecedores ou parceiros, há uma paragem operacional, podem vir multas em cima e, portanto, há uma questão financeira. Não consigo dissociar, mas claramente existe uma importância a nível interno e a nível externo. Aquilo que estamos a assistir

– e que eu acho que é a tendência – é que, cada vez mais, as pessoas vão comprar a organizações que sintam que lhes dão produtos e serviços seguros e confiáveis. E, cada vez mais, as empresas vão contratar fornecedores que também lhes deem o conforto e a garantia – até porque os próprios regulamentos a isso vão obrigar – de que estas empresas têm aplicadas as medidas e os controlos de segurança necessários para prevenir que sejam também uma porta de entrada e um vetor de ataque.

Q9: Agora, gostaria de falar sobre medidas de segurança. Quais considera ser as medidas ou ações que as organizações devem implementar em situação de ciberataque, sobretudo para prevenir a sua ocorrência?

MA: Mais uma vez, vai depender de empresa para empresa, porque tem que ver com os ativos que a empresa quer proteger. Ainda assim, há um conjunto de ações que devem ser tomadas. É importante que as empresas apostem na componente de formação e sensibilização, que é fundamental. Devem fazer uma correta avaliação de risco, precisamente para perceberem qual é o risco a que estão expostas e perceberem quais são os ativos sobre os quais têm de agir. É importante também ter um correta gestão e controlo de identidades e de acessos, como, por exemplo, políticas de *passwords* fortes, ter mecanismos de *multi-factor authentication*… É necessário também terem a capacidade de irem monitorizando para identificar possíveis ataques ou possíveis ações de atividades de risco. Terem um mecanismo de *backups* seguros, portanto segregados daquilo que é a rede principal, que não permitam também a adulteração ou que sejam comprometidos através de um determinado tipo de ataque. É importante que as empresas se dotem dos controlos de segurança que são necessários para tentar antecipar e identificar um possível ataque, agir e conter esse ataque e recuperar de um ciberataque.

Q10: Relativamente a tendências, acho que o Mauro já me falou de algumas. Ainda assim, pergunto-lhe se quer acrescentar mais alguma tendência ou desafio na área da cibersegurança que considere importante mencionar.

MA: Eu diria que o principal desafio, sem dúvida alguma, é a falta de capacidade humana e de conhecimento de cibersegurança nas organizações, seja no panorama nacional como no internacional. Ou seja, há uma grande necessidade de conhecimento tecnológico e profissionais de cibersegurança e há uma grande escassez desses profissionais a nível mundial. Portanto, eu diria que esse é o principal problema das organizações a curto-médio prazo.

Q11: E a nível de tendências, o que considera que irá marcar a área da cibersegurança nos próximos anos e ter uma maior influência no aumento dos ciberataques?

MA: Eu diria que são as tecnologias emergentes. Começo por falar do 5G. Se olharmos para aquilo que foi a transformação digital que houve com a evolução para o 3G e depois para o 4G, estamos a falar de um aumento de banda larga brutal e, para o 5G, irá acontecer a mesma coisa. Portanto, isto vai permitir que haja muito mais dispositivos interligados, muito mais comunicação entre estes dispositivos e, portanto, vai permitir, naturalmente, criar aqui novos vetores de ataque para os quais ainda não estaremos totalmente preparados. Depois acho que a *cloud* e o *edge computing* é um tema que, de uma forma natural, temos de estar sensibilizados e acompanhar, porque muda um pouco o paradigma. Não estou a dizer que a *cloud* é mais ou menos segura, muito pelo contrário, acho que mais uma vez depende de caso para caso. Mas, enquanto uma situação *on-prem* tens ali o teu perímetro de segurança e dá mais conforto às organizações ter algo ali físico, que está contido e que está protegido, quando se passa para *cloud* ou *edge computing* há esta desmaterialização e deixa de haver este perímetro de segurança também de uma forma natural. Continuo a achar que, obviamente, os benefícios superam os riscos, mas este tema de transição para a *cloud* tem de ser tratado com uma estratégia clara e nunca descurando a componente de segurança. Depois temos também a computação quântica. A cibersegurança está muito assente naquilo que são os algoritmos e as técnicas criptográficas atuais, por isso tem existido sempre uma evolução em termos da dimensão das chaves e dos algoritmos que são utilizados… Mas todos eles se baseiam na premissa de que, num tempo considerado seguro, não é possível replicar aquela função criptográfica ou quebrar aquela cifra. Com a computação quântica, os algoritmos existentes podem, com relativa frequência, ser quebrados por utilização de computação quântica numa janela temporal que já não é considerada segura. A Inteligência Artificial também, obviamente, porque começa a haver esta democratização e estar ao acesso de todos. Acho que vai ser um *game changer* também, porque é uma solução tecnológica que está também à disposição dos atacantes.

Q12: Por último, gostaria de saber a sua opinião relativamente ao futuro dos ciberataques em Portugal.

MA: Eu ainda estava na universidade, perto ali do ano de 2000 e pouco, e lembro-me de um professor meu de criptografia aplicada referir precisamente que isto é sempre um jogo do gato e do rato. E a verdade é que isso ainda hoje se aplica. Portanto, eu acho que os ciberataques vão-se tornar cada vez mais criativos e avançados tecnologicamente, vai haver uma tendência de aumento constante… Em alguns momentos, vai haver situações, como crises nacionais ou internacionais, que vão intensificar esse nível de ataques. Mas este aumento crescente vai ser também acompanhado por uma crescente sensibilização e aumento do nível de maturidade das

organizações e capacidade de identificação, mitigação e recuperação de ciberataques. Portanto, vai ser sempre algo contínuo e em paralelo.

Apêndice 4: Entrevista Pedro Mendonça

Q1: Gostaria que o Pedro me falasse um pouco sobre a sua experiência na área da Cibersegurança.

Pedro Mendonça (PM): A minha chegada à Cibersegurança faz-se de um caminho menos frequente ou menos comum. Portanto, eu venho das Ciências Sociais e da área da investigação e do ensino superior, mas a minha investigação no âmbito das Ciências Sociais foi sempre relativa à relação entre as tecnologias digitais e a sociedade, assim num sentido mais lato. Trabalhei também sempre em cruzamento sempre com as dimensões da comunicação, curiosamente. É pela via da experiência nesse tipo de investigação que acabo por vir para o Centro Nacional de Cibersegurança, desenvolver o nosso Observatório de Cibersegurança e colaborar na sensibilização, no desenvolvimento de conteúdos e noutras coisas que acabam por acontecer também. Portanto, o Observatório, que é a minha principal atividade no Centro Nacional de Cibersegurança, procura desenvolver estudos e relatórios sobre a cibersegurança numa perspetiva multidisciplinar e, portanto, também combina bem com essa questão da comunicação. Ou seja, a cibersegurança não é só uma questão de tecnologia e de informática – ainda que seja a dimensão mais basilar –, mas é necessária também a dimensão comunicacional, a dimensão comportamental, a dimensão jurídica, a dimensão económica, as políticas públicas, etc. Portanto, é esta visão multidisciplinar que eu acabo por integrar na cibersegurança.

Q2: Como descreve a evolução dos ciberataques em Portugal?

PM: Relativamente à evolução, eu não tenho uma resposta clara e suficientemente segura a longo prazo. Ou seja, a questão da cibersegurança coloca-se a partir do momento em que há *Internet* – embora ela não se reduza à dimensão da *Internet* –, dispositivos digitais… Nos primórdios, a preocupação da cibersegurança não era muito evidente e ela vai surgindo depois com o tempo. Os anos 80 eu diria que é uma época, a nível internacional, em que a cibersegurança começa a ganhar cada vez mais relevância, nos anos 90 ainda mais e, por aí fora, vai havendo sempre um crescendo. Portanto, a cibersegurança foi ganhando importância. Primeiro, as grandes ameaças eram programas maliciosos que, ainda hoje, são uma grande ameaça, mas depois começa também a evoluir para a dimensão do fator humano, cada vez mais presente, nomeadamente, com os ataques de *phishing* – que é algo que começa a evoluir a partir dos anos 90. E Portugal, tradicionalmente, chega sempre depois a estas coisas, mas quando chega, chega da mesma forma que os outros,

obviamente. Portanto, eu não tenho uma resposta rigorosa relativamente à história da cibersegurança em Portugal em termos dos ciberataques. Mas relativamente aos últimos anos, eu tenho uma noção, precisamente fruto do trabalho dos relatórios que vamos produzindo no Observatório. Uma coisa que eu sei é que o número de incidentes e o registo de cibercrimes aumenta de ano para ano e tem dois tipos de problemas. Temos um problema que tem uma vertente quantitativa elevada, ou seja, acontece com muita frequência, que são, por exemplo, os ataques de *phishing*, *smishing* e *vishing* que estão a crescer bastante, mas temos também as burlas *online*. Eles têm também um impacto distribuído na sociedade e podem atacar qualquer cidadão. Mas depois temos ataques que são menos frequentes, mas que têm um grande impacto nas organizações e podem ter um impacto também relevante nas infraestruturas digitais e nos serviços essenciais. Por exemplo, o *ransomware* é um caso muito relevante deste ponto de vista. E outros ataques que são disruptivos, ou seja, que provocam grandes danos. É o caso, por exemplo, do ataque à Impresa ou à Vodafone, que não resultaram num pedido de resgate, mas simplesmente numa disrupção. Isto são coisas relevantes que vão acontecendo nos últimos anos. O comprometimento de contas também é algo muito relevante, que está diretamente ligado ao *phishing*, ou seja, a captura de credenciais ou *passwords* conduz depois ao *phishing*. Portanto, eu diria que há aqui estes dois grandes vetores: o vetor de quantidade orientada ao fator humano e o vetor impacto orientado às tecnologias. Mas há aqui uma impressão que eu não quero dar, que é o facto de muitos destes incidentes que conduzem a um grande impacto, que têm que ver com *ransomware*, também começam com o fator humano. Ou seja, alguém que clica onde não deve, alguém que partilha uma *password* com quem não deve ou até alguém que autoriza, sem querer, o acesso de terceiros a uma conta privilegiada, por exemplo, através do múltiplo fator de autenticação que, às vezes, não é suficientemente seguro, porque as pessoas autorizam quando não devem. Portanto, eu diria que estes são os grandes aspetos. E depois vamos sendo influenciados por grandes tendências em termos de cenários de ameaças. Tivemos a Covid-19 que foi um cenário muito específico, que provocou efeitos no fator humano, em particular. Portanto, as pessoas isoladas em casa, muito dependentes dos dispositivos técnicos e digitais… Houve um oportunismo por parte do cibercrime relativamente a essas vulnerabilidades. E depois tivemos a emergência da guerra na Ucrânia, que tem características muitos específicas, ou seja, atores estatais que procuram recolher informação e fazer ciberespionagem, *hacktivistas* que procuram criar efeitos disruptivos nos sistemas para chamar a atenção para uma causa… E agora podemos dizer que pode estar a emergir uma tendência que também deve ser considerada que é a Inteligência Artificial, que facilita o acesso de terceiros, não especializados, a instrumentos para realizar ações maliciosas no ciberespaço, como desinformação ou, mesmo até, programas maliciosos.

Q3: Sensivelmente desde 2020, temos vindo a assistir a um aumento significativo do número de ciberataques em Portugal. Quais considera ser os principais fatores que motivaram este aumento? Já me falou da pandemia e da guerra, por exemplo, mas quer acrescentar mais algum?

PM: A pandemia é, certamente, uma das causas. E atenção, algumas das coisas que eu vou dizer são mais comprovadas e outras têm um carácter mais hipotético. Porque as causas na cibercriminalidade nem sempre são fáceis de identificar. É uma dimensão onde a camuflagem é muito fácil de realizar. Portanto, a atribuição de causas é muito difícil. Mas conseguimos tipificar algumas coisas. A verdade é que a pandemia é, certamente, uma causa. Houve um aumento, na ordem dos 80%, dos incidentes registados pelo Centro Nacional de Cibersegurança em 2020. Teve que ver com a pandemia, sem dúvida. E isso teve que ver, certamente, com o oportunismo do cibercrime relativamente a uma circunstância em que havia mais dependência digital e em que as pessoas estavam mais isoladas. Eu diria, portanto, o oportunismo do cibercrime e a maior dependência digital. Mas há outras causas que estão ligadas a isto e que acompanham a tendência geral, que é o facto de utilizarmos mais a *Internet*, os dispositivos digitais… E, portanto, estamos mais expostos aos riscos. E quem realiza os ataques também aproveita mais essa fragilidade. Por outro lado, o cibercrime, os atores estatais, os ativistas e outros vão-se tornando mais sofisticados, vão-se tornando mais profissionalizados e, portanto, aproveitam as oportunidades com mais facilidade. Um terceiro aspeto que eu diria que é relevante – e esta é uma hipótese que eu acho que requer ainda alguma confirmação e que, por exemplo, a pandemia pode ter provocado – é a conversão de algum crime que, tradicionalmente, era *offline* para *online*. Imaginemos as burlas. Imaginemos grupos organizados em Portugal que realizassem burlas, antigamente, a pessoas de idade isoladas nas aldeias. Se calhar agora encontraram no *MB Way*, no *WhatsApp*, nas vendas no OLX uma oportunidade nova para realizar esse tipo de ataques. Porquê? Porque não precisam de sair de casa, têm uma capacidade de massificação muito maior… Eu posso enviar *e-mail* para 100 mil pessoas, basta 1% cair para já ter sido positivo. Eu acho que estes podem ser fatores aqui relevantes. Por exemplo, em Portugal, nós usamos muito mais as redes sociais do que noutros países, do que a média da União Europeia. Também estamos mais expostos desse ponto de vista. Mas esta é uma tendência internacional, não é só em Portugal.

Q4: Agora gostaria que o Pedro me falasse sobre o atual panorama de ciberataques em Portugal. Ou seja, quais os tipos de ataque mais frequentes, os setores de atividade mais vulneráveis e, ainda, os riscos inerentes mais verificados nas organizações.

PM: Relativamente aos incidentes de cibersegurança, o mais frequente é, sem dúvida, o *phishing*. Mas não quer dizer que todo o *phishing* tenha resultados, porque nós registamos o *phishing*

independentemente de ele ter sucesso ou não. E o que registamos não é o *e-mail*, é o URL falacioso. Mas o *phishing* é, sem dúvida, o "campeão" dos incidentes, que afeta o fator humano, em particular. Ao nível do crime, é a burla informática. E estas duas coisas são diferentes, embora estejam correlacionadas, porque são registadas de maneira diferente. O cibercrime é registado pelas autoridades criminais e tem de estar tipificado numa lei, enquanto o incidente é registado pelas equipas de resposta a incidentes das organizações e do Centro Nacional de Cibersegurança. As duas coisas estão correlacionadas, mas os conceitos são diferentes e, às vezes, não têm uma correlação direta, mas indireta. Tem aumentado o *ransomware*. O comprometimento de contas, como eu disse, também é relevante. A exploração de vulnerabilidades técnicas também é relevante. A negação de serviço distribuída também tem aumentado. E outras formas de engenharia social, como, por exemplo, alguém telefonar a outro em nome da Microsoft e conduz a pessoa a instalar um programa malicioso. Quanto aos setores de atividade, temos a banca, ou seja, os clientes da banca, através do *phishing*, são muito atacados. A banca em si tem muita maturidade ao nível da cibersegurança, tem uma grande capacidade de defesa e de resposta. Mas os clientes estão mais suscetíveis, digamos. A saúde também é um setor relevante. A administração pública também. Nos últimos anos, em particular, as câmaras municipais têm sofrido alguns ataques. A educação também regista alguns incidentes. Mas também há alguns setores que registam muitos incidentes, porque têm capacidade de os registar.

Q5: E relativamente aos impactos que os ciberataques podem ter nas organizações?

PM: O grande impacto nas organizações é o *ransomware*, porque paralisa a organização, obriga a organização a colocar a hipótese de pagar o resgaste… Portanto, o *ransomware* é particularmente relevante. Um outro aspeto é a exfiltração de dados, portanto o comprometimento de dados pessoais de clientes, fornecedores e colaboradores e depois como é que esses dados são utilizados pelo cibercrime ou, até, por agentes estatais que queiram utilizar dados com um valor sensível. Portanto, eu diria estes dois aspetos, ou seja, a disponibilidade, confidencialidade e integridade dos dados e depois também a disponibilidade das infraestruturas e dos serviços digitais. Estes são os grandes riscos, digamos, que as organizações enfrentam.

Q6: Já temos vindo a falar muito sobre esta questão, mas qual considera ser a importância de uma organização segura? Ou seja, o que assegura e o que previne.

PM: Uma organização que aposte na cibersegurança, evidentemente, reduz o risco de sofrer um incidente de cibersegurança. O risco não passa para zero, mas é reduzido, é mitigado. Mesmo que nós não consigamos eliminar a hipótese de sofrer um incidente, é muito importante termos a capacidade de recuperar do incidente. Os dados mostram muito que, por exemplo, a grande

dificuldade que as PME's têm, em Portugal, é recuperar do incidente, é voltar a colocar os serviços disponíveis para os clientes e para os colaboradores. Portanto, é muito importante que elas apostem na cibersegurança. E aposta-se em quê? Em três coisas que nós, tradicionalmente, designamos. Primeiro, a tecnologia, ou seja, as organizações têm de ter *firewalls*, múltiplo fator de autenticação, VPN's, antivírus, têm de segmentar as redes… Em segundo lugar, têm de formar as pessoas, porque eu posso ter a melhor tecnologia, mas se algum trabalhador clica num *link* não valeu de nada eu ter apostado na melhor tecnologia. Portanto, as pessoas têm de ser formadas e tem-se de escolher uma cultura de continuidade, ou seja, a cibersegurança não pode ser uma ação de formação que se tem uma vez por ano, aquela coisa chata das *passwords*. Tem de ser uma cultura instalada. Em terceiro lugar, os processos, ou seja, tem que haver análise de risco, tem que se testar as pessoas e as tecnologias, tem que se ter políticas de cibersegurança. E depois a organização, fruto da sua circunstância e do setor a que pertence, tem também que obedecer e seguir as regras legais que estiverem designadas para ela.

Q7: Falou-me sobre a formação dos colaboradores. Qual considera ser o atual grau de preparação das organizações portuguesas em cibersegurança?

PM: Definir um grau não é fácil. Mas as organizações, em geral, têm agido de uma forma muito positiva. Portanto, há uma evolução positiva, sem dúvida. Ao nível das políticas públicas e a nível institucional, nós estamos muito bem classificados a nível internacional. Qual é o grande problema? É a capacitação humana, diria. E há uma falta de recursos, por exemplo, nas PME's em termos financeiros. Mas a capacitação humana dos recursos humanos, melhor dizendo, instalados e a especialização dos recursos especificamente alocados à cibersegurança. Precisamos de mais especialização e de mais especialistas. Esse é um grande desafio para o futuro, diria.

Q8: O Pedro já me falou de algumas medidas e ações que as organizações devem implementar em situação de ciberataque. Quer acrescentar mais alguma, sobretudo para prevenir a ocorrência do ciberataque?

PM: Primeiro, devem identificar quais são os dados críticos que têm, devem conhecer a sua organização. Devem fazer análises de risco relativamente a esses dados críticos e às ameaças que, normalmente, afetam essa organização, para depois priorizar aquilo que é importante e o aquilo que não é importante. Devem ter *backups* da informação mais crítica, é essencial. Devem ter o múltiplo fator de autenticação ativado. E devem formar os seus colaboradores. Ao mesmo tempo, devem segmentar as suas redes também… Agora isto vai tudo depender da dimensão da organização. Se for uma organização muito grande e com funções críticas e essenciais na sociedade, deve ter uma equipa de resposta a incidentes, deve ter uma equipa de operações de

segurança, que vai detetar ameaças. Como disse, vai depender da dimensão e do grau de criticidade dos seus dados. Mas, por exemplo, uma PME deve, pelo menos, ter um *backup* da sua informação e ter o múltiplo fator de autenticação ativado junto dos seus colaboradores.

Q9: Visto que o Pedro está ligado, também, à área da comunicação dentro do próprio Centro Nacional de Cibersegurança, qual considera ser a importância da comunicação numa situação de ciberataque?

PM: A comunicação é uma dimensão que mostra como, de facto, a dimensão de um incidente não é só uma questão técnica. É importante informar e comunicar com os vários *stakeholders* e, como sabe, isso exige diferentes canais, diferentes mensagens – ainda que coerentes entre si –, controlo da narrativa, organização interna entre departamentos que, às vezes, vêm de mundos muito diferentes. Por exemplo, o departamento de IT e o departamento de comunicação precisam de se encontrar a meio caminho. Portanto, tentando simplificar, o fundamental é: comunicar a verdade, comunicar com cuidado – ou seja, não dizer aquilo que não se sabe –, manter os clientes informados, se for o caso, sobre a questão dos dados pessoais, manter as autoridades informadas e manter uma colaboração constante com essas entidades. É melhor o risco da exposição do que o risco da ocultação. E depois também é preciso educar – e isso é um trabalho que o Centro Nacional de Cibersegurança tem de fazer – os *media* e o jornalismo para os temas da cibersegurança. O jornalismo gosta do tema da cibersegurança, mas, por vezes, pode procurar mais o grande efeito e menos a informação adequada. Mas isso acontece em muitos setores, não é só com a cibersegurança.

Q10: Relativamente a tendências e desafios, quais aponta como sendo os mais relevantes na área da cibersegurança?

PM: A emergência de novas tecnologias que introduzem complexidade no sistema e maior capacitação, como, por exemplo, a Inteligência Artificial, o 5G, a computação quântica, a *Internet of Things*… De maneiras muito diferentes, algumas destas tecnologias podem, por um lado, promover capacitação, como a computação quântica, o 5G ou a Inteligência Artificial. Por outro lado, trazem novas vulnerabilidades, novas camadas de complexidade, mais sofisticação aos ciberataques e aumentam a superfície de ataque, como é o caso da *Internet of Things*. A complexidade é um dos grandes desafios da cibersegurança. Como é que, por exemplo, uma empresa como a Microsoft tem de ter, quase todas as semanas, atualizações de segurança aos seus sistemas? Acontece porque o sistema de raiz não estava suficientemente seguro. Isso acontece também, por sua vez, porquê? Porque é muito complexo, porque tem muitas linhas código. Portanto, mesmo uma grande empresa como esta não controla totalmente o nível de complexidade

do seu produto. E depois há ainda um outro aspeto, que são as dimensões geoestratégicas. O ciberespaço é um espaço de ação também dos Estados e da ação tradicional dos Estados a este nível, não é só para o cibercrime, é também para os Estados que fazem ciberespionagem, que podem fazer ações disruptivas, etc.

Q11: Por último, gostaria que o Pedro me desse a sua opinião relativamente ao futuro dos ciberataques em Portugal.

PM: É uma pergunta difícil, porque esta é uma área muito incerta. Contudo, o que nós vemos a acontecer tem que ver com aquilo que eu estava a dizer há pouco. Há consequências que nós podemos já adivinhar, que tipos de tecnologias emergentes estão associadas. A maior sofisticação dos ciberataques, muito relacionados com a Inteligência Artificial, em que cada vez mais se vai cruzar a dimensão técnica do ciberataque com a perceção humana, nomeadamente na criação de conteúdos de desinformação. Portanto, aquilo que se fala que são as ameaças híbridas, isso cada vez mais vai acontecer. Pode haver um país a ser atacado por outro ou alguém a atacar alguém, em que, por um lado, realiza um ataque de negação de serviço, um *phishing* e, ao mesmo tempo, uma campanha de desinformação. Isto tudo pode ser possível com a Inteligência Artificial, por exemplo, na campanha de desinformação, nomeadamente. E podemos até – isto é uma hipótese que eu lanço que me parece interessante –, com a Inteligência Artificial, encontrar uma ameaça em sistemas de Inteligência Artificial que, de forma involuntária para o ser humano, escapem aos mecanismos de decisão humana, ganhem autonomia suficiente e comecem a produzir efeitos maliciosos no ciberespaço, de uma forma autónoma. Podemos imaginar uma coisa destas. Infelizmente, não é assim tão ficção científica. Mas eu acho que uma tendência que nós podemos ver é precisamente isso, uma combinação entre ameaças atípicas da dimensão de perceção com ameaças mais técnicas.

Apêndice 5: Entrevista António Gameiro Marques

Q1: Gostaria que o António me falasse um pouco sobre a sua experiência na área da Cibersegurança.

António Gameiro Marques (AM): Tenho uma formação muito ligada à área das Tecnologias da Informação e da Comunicação. Portanto, a segurança da informação sempre me acompanhou desde muito cedo e a cibersegurança é, conceptualmente, uma disciplina da segurança da informação. É preciso ter em consideração que a segurança da informação é todos os processos, tecnologia e pessoas que acautelam que a informação, quando é tramitada, os processos garantem a confidencialidade, a integridade, a disponibilidade e o não-repúdio da informação. E a

cibersegurança, depois, verticaliza este conceito quando o digital entra nas tecnologias da informação. Portanto, eu acompanho isso desde bastante cedo na minha vida profissional. Depois, já neste século, quando estou a prestar serviço na NATO como conselheiro do senhor embaixador de Portugal junto da NATO, sigo estes temas e, em 2007, estou lá quando ocorre o ataque que foi marcante na história da NATO. E porquê que foi marcante? Porque foi um evento que foi motivado por razões políticas. Como saberá, foi no decorrer de uma decisão das altas autoridades daquele país que retiraram uma estátua de um soldado russo numa zona nobre da cidade para uma outra zona menos conhecida e a comunidade russa, em retaliação, desencadeou com todos os seus pares na Rússia e outros "amigos" um ataque em abril/ maio de 2007 que levou a que a história passasse um mau bocado durante um período relativamente longo. Quando digo um mau bocado é ao ponto de não se conseguir levantar dinheiro, não se conseguir fazer compras *online*, faltar combustível nas bombas de combustível, hospitais com dificuldades, enfim… Eu estava na NATO quando isso aconteceu e, portanto, acompanhei muito de perto quer o desenvolvimento tecnológico, mas, sobretudo, e isso é que é relevante aqui para a mudança, o tema teve visibilidade política pela primeira vez. E foi aí que a NATO começou a olhar para estes temas, precisamente numa ótica política e, depois, político-estratégica. Portanto, eu acompanhei isso nessa altura, depois venho para Portugal e, após fazer a formação que é a condição necessária para ser promovido a contra-almirante, fui CIO da Marinha na parte da cibersegurança e depois fui Secretário-Geral Adjunto do Ministério da Defesa na parte das tecnologias da informação. Em 2012, faço parte da comissão instaladora do Centro Nacional de Cibersegurança, que é criado em outubro de 2014, fruto dos trabalhos dessa comissão. Depois, a 1 de setembro de 2016, sigo funções enquanto Diretor-Geral do Gabinete Nacional de Segurança, que é a estrutura onde funciona o Centro Nacional de Cibersegurança. O coordenador do Centro, o senhor engenheiro Lino Santos, é o meu Subdiretor-Geral para aquela área e, portanto, o Centro Nacional de Cibersegurança é algo com que lido todos os dias desde 2016, já lá vão quase 7 anos. Portanto, a minha ligação com a cibersegurança é um bocadinho condensada.

Q2: Gostaria que começasse por me falar sobre a evolução dos ciberataques em Portugal.

AM: Publicámos recentemente, no nosso *site*, o relatório Riscos & Conflitos de 2023. É um relatório que documenta muito bem todos os dados relevantes para responder à sua pergunta. Mas, de uma forma geral, o que lhe posso dizer é que os ataques, com a pandemia, sofreram um incremento muito significativo. Esse incremento era enaltecido quando entrávamos em *lockdown*. Portanto, em 2020 tivemos dois momentos de *lockdown*, logo ao princípio, em março e abril, e vê-se, de facto, em gráfico no próprio relatório uma subida, depois uma ligeira descida e depois, mais para o segundo semestre do ano, há um novo *lockdown* e um novo incremento. Os ataques

continuaram a crescer a partir daí, porque as pessoas cada vez tiveram maior contacto com o digital. Nós dizemos que a densidade digital aumentou, o que significa que, por metro cúbico, havia muito mais pessoas ligadas simultaneamente à *Internet*. Portanto, se havia mais pessoas, mais prevaricadores havia, com algumas pessoas que também não têm grandes competências digitais, a verdade é que estavam criadas as condições para que os ciberataques se manifestassem. Ciberataques há sempre, só que há os bem-sucedidos e os menos bem-sucedidos. E porquê que estes eram bem-sucedidos? Porque, inclusivamente, houve muitas pessoas que tiveram de trabalhar a partir de casa, nos seus próprios computadores – não nos computadores corporativos – e isso levava a que, como os computadores em casa não estariam tão protegidos como seria desejável, os *malwares* que estavam nos seus computadores se espalhassem às organizações. Um dos anos que é, de facto, um ano marcante nesta área é 2022. Este ano teve ataques muito mediáticos. Começou, aliás, no dia 2 de janeiro de 2022, com um grande ataque a um grande grupo de comunicação social, que é a Impresa. O ano foi muito profícuo em incidentes muito variados, bastante significativos. Houve 25 grandes incidentes, em Portugal, em 2022, o que significa que houve um bocadinho mais de 2 por mês. Mas foi, sobretudo, um ano de grande aprendizagem. Nós só aprendemos quando, de facto, somos confrontados com a realidade. Podemos aprender teoricamente nas aulas, mas é quando temos de agarrar o problema e ajudar a resolvê-lo que, na verdade, se aprende. Embora tenha sido um ano muito rico em aprendizagem, foi também muito denso em tensão por causa destes incidentes e do impacto que eles tiveram na nossa sociedade.

Q3: O António falou-me do facto da pandemia ter provocado este aumento. Que outros fatores considera que tenham contribuído para este aumento de ciberataques desde, sensivelmente, 2020?

AM: Há um evento que, aparentemente, também provocou um incremento, sobretudo em 2023. Se olhar para o tal relatório que já lhe mencionei, verifica-se que há, na verdade, um crescimento de incidentes muito significativo em 2020, 2021 e 2022, embora o declive da curva ou a velocidade de incremento tenha diminuído. Ou seja, eles continuam a aumentar, mas a reta, em vez de ser muito inclinada, é um bocadinho menos inclinada, o que significa que a velocidade a que estão a aumentar é menor. Uma das razões que é plausível de estar subjacente a isso é a situação geoestratégica que se vive atualmente. Há uma tensão clara no mundo físico, que se manifestou em guerra com a invasão da Ucrânia pela Rússia e, logo aí, deu origem, direta ou indiretamente, a uma proliferação de ataques – embora o relatório Riscos & Conflitos 2023 não faça uma correlação direta entre uma coisa e outra, é algo que eu contesto. Mas depois há outros focos de tensão geoestratégica no mundo. A China e os Estados Unidos da América por causa de Taiwan, por causa das questões comerciais e essa tensão depois tem expressão no ciberespaço, como todos os

incidentes que se estão a manifestar. E depois, quem prevarica e consegue obter fundos através de *ransomware* já percebeu que, entretanto – transformado o *ransomware* como negócio, o *ransomware as a service* –, há entidades, que funcionam quase como empresas, que depois fazem ataques muito sofisticados, levando ao recebimento de verbas em criptomoedas que, depois, são usadas para financiar outras coisas ilícitas, como o terrorismo. Tudo isto, conjugado, faz com que, na verdade, os ciberataques tenham aumentado, embora, repito, com uma velocidade ligeiramente menor.

Q4: Gostaria que o António me falasse sobre o atual panorama de ciberataques em Portugal, ou seja, quais os tipos de ataque mais frequentes, os setores de atividade mais vulneráveis e, ainda, os riscos inerentes às organizações mais verificados.

AM: Mais uma vez, no relatório Riscos & Conflitos tem lá esquematizado quais são os ataques mais comuns. Na taxonomia, nós indicamos a fraude e classificamos a fraude uma série de eventos ou de incidentes. Relativamente às áreas de atividade, eu diria que a administração pública, prestadores de serviços essenciais, como saúde e educação, e prestadores de serviços digitais estão, normalmente, no topo, porque também são muito mais expostas. Quanto aos riscos, por exemplo, aqueles ataques que ocorreram em 2022 provocaram a indisponibilidade de serviços, quer da própria empresa, quer das empresas por elas servidas. Por exemplo, a Vodafone esteve com os serviços indisponíveis durante cerca de 8 dias e isso teve um impacto significativo na performance da empresa. Felizmente, não teve impacto na cotação bolsista, porque eles geriram muito bem o incidente, conseguiram recuperar, conseguiram restabelecer a confiança dos seus clientes. Há um tempo, eu vi a diretora de marketing da Vodafone falar do incidente e percebi que não houve clientes que tivessem mudado a Vodafone para outro *provider* por causa do incidente, porque, na verdade, eles geriram muito bem. Mas houve impactos significativos, veja o Hospital Garcia de Horta, que teve que recolocar alguns doentes, teve consultas paradas, conseguiu não parar as urgências com uma instalação de computadores específica para aquela situação… A Germano de Sousa que também teve uma gigante deturpação de dados. Nós não temos conhecimento, pelo menos em Portugal, de entre estas empresas que sofreram grandes ataques, de falências de organizações por causa de ciberataques. Agora que tem impacto na performance da empresa, que é quantificável em euros, isso tem. Ainda há pouco tempo, soube de uma empresa que teve um ataque de *ransomware* grave, conseguiram recuperar, mas todo o tempo que tiveram de resolver o problema e mais a empresa que tiveram de contratar para os ajudar a recuperar teve, depois, manifestações no seu balanço, porque foi investimento que tiveram de fazer, quando deviam era estar a vender serviços e produtos e, assim, a ganhar dinheiro. A mim parece-me que é por causa disto que as pessoas acabam por, ainda que levando a cibersegurança cada vez mais a sério, não a

levar tão a sério como isso, porque os ataques confinam-se iminentemente à área do IT e não ao OT. *Information Technology* (IT) é aquilo que todas as organizações têm: a sua rede, os seus sistemas de gestão de pessoas, salários, património, logística, área financeira. O *Operational Technology* (OT) é as tecnologias de informação e comunicação que são usadas para controlo de fábricas ou de dispositivos industriais. Por exemplo, uma barragem é controlada através de um sistema OT que, no fundo, é um computador específico concebido para aquele propósito, que depois tem uma matriz enorme de sensores que mede o ambiente. Ora, há ataques a sistemas OT e o mais famoso, talvez, é o ataque ao sistema da fábrica de enriquecimento de uranio do Irão, o Sutxnet. O que sucedeu foi que foi planeado um ciberataque a esta fábrica, com o objetivo de produzir uma arma nuclear. Os *hackers* introduziram um *malware* que fez com que as centrifugadoras, que têm de rodar a uma velocidade controlada para não se partirem, vissem comprometido o mecanismo de controlo da velocidade e acelerassem até partirem. Esse foi, talvez, o ataque mais significativo nos últimos anos, através de um sistema OT. O comprometimento a um sistema OT pode ser fatal.

Q5: De forma geral, já temos vindo a falar sobre esta questão, mas qual considera ser a importância de uma organização segura? Ou seja, o que assegura e o que previne à organização uma maior aposta na cibersegurança.

AM: Para começar, o nosso mundo real tem uma componente física e uma componente virtual. Cada vez mais, o nosso mundo tem uma maior componente virtual por causa do digital e nas empresas é a mesma coisa. Aliás, há empresas que só nasceram por causa do digital, como Netflix, PayPal, Meta… Todas essas empresas nascem porque existe o digital e, portanto, enquanto existir digital, aquelas empresas existem. Nós próprios, seres humanos, vivemos nas duas dimensões e uma grande parte das nossas empresas vivem nas duas dimensões. Ora, se no mundo real uma empresa arranja cercas físicas à sua volta, tem controlos de entrada, sistemas para prevenir contra incêndios, então também tem de ter no mundo digital mecanismos que promovem a segurança, ou seja, a cibersegurança. É um raciocínio perfeitamente lógico, tendo por base esta dualidade do mundo real em que vivemos. Agora, há empresas que têm, por via da lei, obrigações específicas. E quem são essas empresas? São as empresas que são designadas pela Diretiva NIS, como sendo operadores de serviços essenciais, prestadores de serviços digitais e operadores de infraestruturas críticas. Essa Diretiva foi transporta para a nossa lei nacional na lei n.º 46, de 13 de agosto de 2018. No anexo a essa lei, estão todas as áreas da sociedade que têm prestadores essenciais, sendo que no nosso país são cerca de 450. Na Diretiva NIS 2, que já foi aprovada em dezembro de 2022 e vai ser transposta para a nossa legislação até outubro de 2024, os critérios são mais precisos, portanto o que nós antecipamos é que o número de operadores de serviços essenciais diminua.

Mas, mesmo assim, há empresas que têm de cumprir um conjunto de requisitos de cibersegurança. Em resumo, hoje em dia, é difícil que alguma entidade, seja pública ou privada, diga que não tem de ter cuidados na área da cibersegurança. E mais, a lei obriga a que algumas dessas entidades, ao nível de empresas ou administração pública, cumpram um conjunto de requisitos mínimos de cibersegurança.

Q6: Qual considera ser o atual grau de maturidade das empresas portuguesas em cibersegurança?

AM: Há empresas no nosso país que já têm níveis de maturidade bastante significativos. E têm-no porque, mesmo antes da tal lei n.º 46 que eu há bocado lhe disse, já o tinham devido à sua exposição quer ao IT, quer ao OT. Estou a falar de uma E-REDES, de uma Galp, de uma Sonae, uma Vodafone, uma Altice… empresas desta dimensão, mas mesmo assim foram atacadas. Qual é a diferença que nós constatámos em 2022 em face disto? Isto é um aspeto importantíssimo a reter. As empresas que foram atacadas e que estavam bem preparadas, recuperaram num tempo finito e não perderam informação. Conseguiram recuperar tudo, só não recuperaram o tempo que perderam na fase de recuperação. As outras que não estavam preparadas, ou tão bem preparadas, não só perderam informação para sempre, como não conseguiram recuperar completamente, ou seja, houve sistemas e serviços que não voltaram a ser repostos. Veja o quão dramático é uma empresa com 30 ou 40 anos perder informação para sempre. É a mesma coisa que uma família, que já tem muitas gerações, de repente tem um incêndio em casa e perde todas as fotografias da família, os documentos do tetravô e do bisavô… quer dizer, perde uma parte significativa da sua identidade. Porque a informação contribui para a identidade do conjunto. Portanto, as empresas, de facto, tiveram essa diferenciação. Em relação à questão que me colocou, eu sistematizaria naquelas que estão bem preparadas e que estão maduras e, por isso, mesmo sob ataque, conseguem reagir, e depois há aquele conjunto de empresas, que é a maioria, que não está bem preparado. É por isso que nós insistimos tanto na formação e na capacitação. Aliás, a Estratégia Nacional de Segurança do Ciberespaço, aquela que ainda está em vigor, tem um eixo que é o eixo 2, da capacitação, onde a maior parte das iniciativas dos diversos planos de ação que temos tido ao longo da vigência da estratégia estão na capacitação das pessoas, a começar pela sensibilização, alertando para os problemas. No CNCS, temos também a iniciativa *C-Academy*, que visa formar 9800 profissionais de cibersegurança até 2026, através de uma rede de todos os politécnicos e universidades públicas do nosso país. Portanto, é uma iniciativa de formação nacional e tentacular a todos os distritos e capitais de distrito do nosso país. Esta iniciativa não vai dar nenhum grau académico, mas dá microcréditos que, por acumulação, pode fazer a diferença na candidatura a licenciatura ou mestrado nessa área.

Q7: Quais considera ser as principais ações e medidas de cibersegurança que as organizações devem implementar, sobretudo para prevenir a ocorrência de um ciberataque?

AM: O que nós recomendamos é que as empresas usem o nosso quadro, o Quadro Nacional de Referência em Cibersegurança, associado a um roteiro para a maturidade em cibersegurança e o sigam como guião para incrementar a sua maturidade. Mais concretamente, em fins de 2021, desenvolvemos com a Imprensa Nacional Casa da Moeda e com a Secretaria de Estado da Economia e da Transição Digital um conjunto de selos para a maturidade digital em cibersegurança. Para se obter estes selos, é necessário que se cumpra um conjunto de requisitos muito significativos e, caso as empresas os cumpram, já ficam com níveis muito interessantes de cibersegurança. Eu vou-lhe mostrar alguns, numa das várias apresentações que tenho sobre o tema. Como pode ver, já o nível bronze tem este conjunto de requisitos, que nós chamamos controlos, que permitem precisamente que as organizações possam incrementar o seu nível de maturidade. Identificar as funções ou atividades que são críticas e, em função disso, perceber que processos, sistemas de informação e tecnologias de informação estão associados a essas atividades, identificando os seus riscos e o plano de mitigação de riscos. Inventariar os ativos que constituem esses sistemas. Ter uma política de utilização aceitável dos recursos TIC, ou seja, esta política é um documento que qualquer trabalhador da empresa lê e tem de perceber e reconhecer, através de uma assinatura, um conjunto de coisas que pode e não pode fazer. Identificar o responsável pela função de segurança da informação. Ter cópias de segurança fora do domínio. Ter atualizações de segurança regulares. Deve-se ter uma autenticação múltiplo fator, não se deve autenticar só com *username* e *password*, porque, através de mecanismos de *phishing*, essas credenciais são exfiltradas e depois são utilizadas por quem quer fazer mal para entrar na nossa conta. Enfim, há um conjunto de normas que, nós próprios, no *site* do CNCS, aconselhamos que sejam implementadas. Mostro-lhe agora um quadro resumido disso. Como pode ver, em termos de vulnerabilidades mais exploradas, temos o facto de as aplicações estarem desatualizadas. Temos muitas aplicações a funcionar, quer no setor privado, quer no setor público, que são as chamadas *legacy*, ou seja, aplicações cuja tecnologia já nem é acompanhada pelo fabricante. Outra vulnerabilidade é o facto das *passwords* e *usernames* não serem atualizados com regularidade. O facto de ainda haver muitas pessoas que não sabem, portanto temos de investir na sua capacitação e formação. E a própria arquitetura dos sistemas não foi concebida para acautelar precisamente estes ataques. Ao nível de medidas de mitigação, temos, por exemplo, regulamentar o múltiplo fator de autenticação, contratar serviços de anti-DDoS, ter testes de penetração regulares, ou seja, contratar *hackers* benignos que fazem ataques para ver que vulnerabilidades é que a organização tem. Depois devemos ter sempre um registo histórico centralizado, para saber o que é que

aconteceu, ou seja, se houver um incidente no registo histórico, é o nosso passaporte para compreendermos o que se passou. Outra medida é os *backups* estarem *offline* e, por fim, ter um plano de recuperação, ou seja, fomos atacados, temos *backup* bom, então vamos recuperar e temos de ter um plano de recuperação e, naturalmente, termos um parceiro com quem trabalhar para nos ajudar a fazer esse plano de recuperação, para além de um plano de comunicação, porque os nossos *stakeholders* vão querer saber o que se está a passar.

Q8: Quais considera ser as principais tendências e desafios na área da cibersegurança, que promovem o aumento de ciberataques?

AM: Há as tendências que já lhe falei do incremento, embora com menor velocidade, dos ciberataques. O que nós verificamos é que, ciclicamente, os *hackers* vão agarrar em ferramentas antigas e reformulá-las. Ainda hoje li uma notícia que um dos *malwares* mais poderosos, que é o *emotet*, está outra vez a ressuscitar, mas com algumas alterações que faz com que ele passe os sistemas de deteção preventiva. Portanto, ataques mais sofisticados, isso dá-me a ideia de que vai ser uma tendência, quanto mais não seja porque a tecnologia também está a evoluir e uma coisa está sempre associada à outra. Depois há uma tendência, que é um desafio, que é nós acompanharmos a tendência regulatória da União Europeia. Há uma pressão grande com a NIS 2 e com a *Critical Entities Resilience Directive*, que é também um diploma, uma diretiva da União Europeia que vai estabelecer um conjunto de requisitos. Depois há uma tendência também para, progressivamente, as pessoas estarem mais letradas do ponto de vista digital, ou seja, a literacia digital irá aumentar e, ao aumentar, também vem com ela uma maior sensibilidade e alerta para situações que podem levar a que os seus sistemas sejam comprometidos. O problema é que numa organização de 200 pessoas, basta que uma faça clique num *link* errado para comprometer toda a organização. Por isso, é absolutamente importante, para não dizer fundamental, investir na formação das pessoas.

Q9: Por último, qual considera ser o futuro dos ciberataques, sobretudo em Portugal?

AM: Eu não diria só em Portugal, porque não há algo específico só em Portugal e já deve ter ouvido, inclusive, que o ciberespaço não tem fronteiras. O que nós temos é definido o conceito de ciberespaço de interesse nacional, que está definido na Estratégia Nacional de Segurança do Ciberespaço. O ciberespaço de interesse nacional é aquele ciberespaço onde se jogam interesses nacionais. Por exemplo, imagine uma fábrica importante portuguesa que tenha uma implantação no México e, se for atacada e tiver de parar a produção, estamos a falar de uma empresa privada, mas que está a impactar os interesses nacionais. Uma embaixada de Portugal num sítio qualquer é, do ponto de vista do direito internacional, um território nacional e o ciberespaço que ela utiliza

é um ciberespaço de interesse nacional. Portanto, estou convencido de que os ciberataques vão começar a ser cada vez mais estimulados pela Inteligência Artificial utilizada para fins maliciosos. Nós temos de contra-atacar, colocando nos sistemas de proteção e de prevenção também Inteligência Artificial. Porque a sucessão com que as coisas estão a ocorrer não se compadece com a velocidade do ser humano e, portanto, a quantidade de informação que recebemos por segundo é tão grande que, se não tivermos sistemas que fazem esse rastreio recorrendo a algoritmos de Inteligência Artificial, não vamos conseguir fazer face aos desafios, porque os *hackers* já o vão fazer. Portanto, eu estou convencido de que a tendência futura vai ser na sofisticação de ataques por via do recurso a algoritmos de Inteligência Artificial. Todas as tecnologias podem ser utilizadas para o bem da humanidade, mas também podem ser usadas de uma outra perspetiva.

Q10: Penso que conseguimos tocar em todos os pontos que tinha previsto inicialmente. Não sei se o António quer acrescentar mais alguma coisa que considere pertinente para o meu trabalho e que não tenhamos abordado.

AM: A Sara disse-me que o seu trabalho é no âmbito do mestrado em Relações Públicas. Quero-lhe dizer que é bastante importante que tenha agarrado este tema, porque uma das componentes muito importantes em situações de ciberataque é a comunicação, a maneira como comunicamos estes temas. Nós temos precisamente profissionais dessa área a trabalhar connosco, porque o cidadão é para quem nós trabalhamos. Mas para os servirmos da melhor forma, temos de ter uma comunicação que qualquer um entenda. Temos de conseguir chegar ao cidadão normal, sensibilizá-lo para estes temas, dar-lhe exemplos, através de uma comunicação cuidada para conseguir chegar a cada pessoa, individualmente. Portanto, temos de ter uma equipa de comunicação, de relações públicas, que entenda isso e traduza essa linguagem em grafismos, em exemplos, em pequenas campanhas. Aliás, há uma campanha em curso até ao fim do mês de julho, que estamos a fazer em colaboração com a Secretaria de Estado da Digitalização e da Modernização Administrativa, que é #LerAntesClicarDepois com pequenos vídeos que vão passando na RTP1, precisamente para dar exemplos às pessoas para os alertar para determinados comportamentos úteis e protetores. Portanto, é uma atividade absolutamente importante, porque, inclusivamente, vamos ter de falar de maneira diferente para um jovem que ainda não entrou na adolescência, para um adolescente, para um adulto em plena idade ativa e para uma pessoa que já esteja na reforma. E têm de ser profissionais dessa natureza que agarram na mensagem que queremos transmitir e a transformam de maneira que ela chegue a mais público.

Apêndice 6: Entrevista Pedro Verdelho

Q1: Gostaria que o Pedro começasse por me falar um pouco sobre a sua experiência na área da Cibersegurança, mais concretamente do Cibercrime.

Pedro Verdelho (PV): Começaria precisamente por esse ponto. A cibersegurança e o cibercrime são duas facetas de uma realidade que pode ser coincidente, portanto duas formas de ver a mesma realidade. Por exemplo, quando há um acidente na estrada porque uma pessoa atropela outra, a primeira preocupação é, evidentemente, chamar uma ambulância para levar aquela pessoa para o hospital, para lhe salvar a vida ou para minimizar as feridas que possa ter. Mas, quando a GNR vai ao local, a principal preocupação é recolher provas daquilo que aconteceu, porque, se houver um crime, tem de haver recolha imediata de indícios no local. Com o cibercrime e com a cibersegurança acontece precisamente a mesma coisa. As pessoas da área da cibersegurança, quando há um incidente, a primeira preocupação é recuperar o sistema, para minimizar estragos. A preocupação da área do cibercrime é recolher informação que permita chegar ao atacante. Uma e a outra podem colidir. Quando um administrador de um sistema a primeira coisa que faz é apagar tudo o que o atacante deixou e pôr o sistema a funcionar, quando chega a Polícia Judiciária está tudo apagado e já não há pistas. Portanto, esta é uma área difícil de gestão, é uma área na qual estamos a dialogar com o Centro Nacional de Cibersegurança há anos, do lado das autoridades de justiça criminal, portanto o Ministério Público coadjuvado pela Polícia Judiciária. Nós estamos a trabalhar com o Centro Nacional de Cibersegurança na conciliação destes dois interesses que são antagónicos. Obviamente que estão ambos do lado da aplicação da lei e a verdade é que um e outro podem colidir no caso concreto. Por isso é que comecei por este ponto, porque, de facto, há uma aproximação diferente entre a cibersegurança e o cibercrime. Eu trabalho em cibercrime desde há muitos anos, temos há muitos anos a necessidade de gerir um ataque informático, mas de uma perspetiva diferente daquela que é gerida pelas autoridades de cibersegurança.

Q2: Qual considera ser a evolução dos ciberataques em Portugal?

PV: Eu acho que é claro, tendo em conta a informação toda que circula e os relatórios oficiais, que o cibercrime está a aumentar. Antes de prosseguir, deixe-me dizer-lhe isto. Se é verdade que cibersegurança é uma coisa e cibercrime é outra, também é verdade outra coisa. Ao contrário do que acontece nos acidentes na estrada, por exemplo, uma violação de uma regra de trânsito não é necessariamente um crime, pode haver um acidente simplesmente por acidente. Isto são acidentes provocados por incidentes. No informático, também podem acontecer incidentes, um disco rígido que aquece de mais e paralisa a conversação, uma ligação à *Internet* que não está eficaz, que congela a nossa comunicação e deixamos de conseguir ouvir-nos... Isto são incidentes. Agora, tal

como na estrada, há atos propositadas e resultado da atividade humana. Contudo, na estrada, a generalidade dos acidentes não são provocados. Na área ciber, a generalidade das violações de regras de segurança são crime, porque a maior parte são deliberadas, é alguém que quer atacar um sistema, alguém que quer mandar um sistema abaixo… Não me estou a referir àqueles pequenos acidentes, esses não têm relevância, acontecem. Mas, ao contrário do que acontece em muitas outras áreas, as violações de regras de cibersegurança normalmente são crime. Acesso ilegítimo a um sistema, para além de ser uma violação a uma regra de segurança, também é crime. Ataque a um sistema informático, para além de ser uma violação de uma regra de segurança, também é crime. Utilizar, mal-intencionadamente, a *password* de outra pessoa é uma violação de uma regra de segurança e, ao mesmo tempo, é um crime. Isto para chegar ao ponto no qual comecei. Ao contrário de muitas outras áreas, na área ciber quase todas as violações de segurança são um crime. Portanto, quase todos os ataques de cibersegurança são um crime. Só aqueles meramente acidentais é que não são crime, que são poucos. Na generalidade das vezes, isto é resultado da ação humana, ação deliberada, intencional, portanto é crime. O que quer dizer que, embora vivamos em mundos diferentes, com interesses diferentes, a comunidade do cibercrime converge no mesmo foco de ação da comunidade da cibersegurança, sobretudo que é em grande escala. Por exemplo, se alguém obtiver a *password* de acesso ao seu *e-mail* trata-se de um problema de cibersegurança, porque vê a sua privacidade invadida, mas não é uma questão preocupante para o mundo da cibersegurança em geral, como são os ataques a grandes estruturas de empresas de comunicação, de empresas de telecomunicações, de bancos ou entidades de serviços públicos. Portanto, vemos casos muito diferentes e a comunicação de umas e de outras também é diferente. Acredito que tenha escolhido este tema para a sua tese por causa dos ataques que ocorreram, sobretudo, no início do ano de 2022, evidentemente, em que a comunicação foi um fator essencial. Em particular, o ataque à Vodafone, que teve na comunicação um elemento essencial e eu acho que a generalidade da comunidade percebe que a comunicação foi muito bem gerida, permitindo-lhes uma maior capacidade de recuperar. Portanto, a questão da comunicação em ataques desta dimensão e desta natureza é uma questão importante, naturalmente, como em qualquer outra questão de segurança, diria. Num ataque terrorista, por exemplo, a comunicação é essencial para deixar as pessoas mais tranquilas. Voltando à sua questão inicial, é sabido que os números de ciberataques estão a subir de uma forma permanente, consistente e constante. Portanto, houve um pico durante a pandemia, mas esse pico já foi completamente ultrapassado, e a verdade é que a pandemia só empurrou alguma digitalização. Sempre houve ataques informáticos, do género desse da Vodafone ou da SIC… quer dizer, não posso dizer que sempre houve, porque antes de haver *Internet* não havia. Este tipo de ataques informáticos que está a pensar são ataques informáticos a sistemas de informação. É um tipo de ataque que começou somente no fim da primeira década deste século,

porque, até aí, a *Internet* não tinha uma utilização massiva, não era utilizada como uma ferramenta diária de trabalho. Por exemplo, o *gmail* é uma realidade de 2005, as pessoas utilizavam-no, sobretudo, por razões institucionais e, portanto, cada empresa tinha um serviço próprio de *e-mail*. E quanto a outros serviços *web*, foi algo que começou por volta do ano 2000, por exemplo, entregar os impostos na *Internet* é algo de 2010, por aí. E só a partir desta altura é que se coloca esta questão dos ataques a sistemas. Já se podia atacar um sistema, mas isso não tinha repercussão, porque as pessoas daquela empresa ficavam com o computador não utilizável durante um dia ou dois, mas não acontecia mais nada. Agora, atacar um sistema informático, por exemplo, de um canal de televisão, ou de um jornal, ou de um banco, isso já tem repercussões em terceiros. Os bancos na *Internet* são um fenómeno do início dos anos 2000 e é nessa altura que começam os ataques a bancos e ataques de várias naturezas, não é só mandá-los abaixo, é até mandar roubar as *passwords*, por exemplo. Quando há uma atividade lucrativa, os bandidos procuram obter dinheiro aí. E nem todos os ataques são ataques de natureza política, de *hacktivismo*. A generalidade deles são para obter dinheiro. Isto tem uma parte completamente verdade e outra parte que não é completamente verdade, que recentemente ganhou dimensão, que é a guerra cibernética. A invasão da Ucrânia pela Rússia tem uma subcamada que nem sempre faz notícia que é a guerra digital também. Antes de a guerra começar no terreno, já a guerra digital tinha começado. Até já houve alguma previsão da guerra no terreno, porque já tinha começado a guerra no digital. Esta é uma realidade importante também, mas tem mais que ver com ciberdefesa e ciberguerra. Na área dos ciberataques não militares, a generalidade das situações tem que ver com dinheiro. O *ransomware*, que é dos maiores problemas hoje em dia, tem em vista obter dinheiro. A generalidade dos DDoS também é para obter dinheiro. E como se trata de dinheiro, neste momento, a generalidade desse tipo de atividades é feita por crime organizado que vive disso. Claramente desde esta década, esta é uma atividade económica florescente e que vem crescendo em massa e, portanto, os problemas de cibersegurança também se colocam a este nível, como reflexo do crescimento em massa dos serviços *online*. Como lhe dizia há pouco, a pandemia só empurrou este fenómeno. A pandemia, por exemplo, fez disparar para números astronómicos os valores de comércio eletrónico. E perante este cenário, os criminosos começaram a explorar possibilidades à volta de toda esta atividade de ganhar dinheiro sem ter de fazer grande esforço. Para resumir, desde há algum anos, muito visível mais depois da pandemia, mas já antes bastante claro, há progressão constante, consistente e permanente dos problemas de cibercriminalidade que decorrem da explosão do digital.

Q3: Falou-me agora da pandemia e da explosão do digital. Que outros fatores considera terem motivado o aumento de ciberataques nos últimos anos?

PV: Eu acrescentaria a falta de literacia digital. Eu acho que esse é um assunto que tem de ser bem sublinhado. Toda a gente, hoje em dia, tem acesso à *Internet* no telemóvel e nem toda a gente sabe, exatamente, no que se está a meter. Por exemplo, há cerca de 100 anos, qualquer pessoa podia conduzir automóveis, porque não havia código da estrada, não havia carta de condução, não havia regras. Na *Internet*, estamos nesse ponto ainda, isto é, qualquer pessoa pode navegar na *Internet*, pode fazê-lo da forma que quiser, não existe nenhuma regra de conduta. Isto significa que, se quiser abrir um *site* na *Internet* para vender pornografia infantil, não há forma de controlar isso. Se quiser abrir um *site* para burlar as pessoas, não há forma de controlar isso. Podemos bloquear em Portugal, somos um estado de direito, mas noutros sítios não. E isto colide, de facto, com as nossas limitações próprias. Pessoas com menos literacia, que vai desde pessoas de idade, a crianças, a pessoas adultas que não têm noção destas realidades, que não estão sensibilizadas para elas, caem facilmente em burlas, por exemplo. Portanto, a pandemia não foi uma causa, mas foi o que empurrou o que já estava em marcha antes. E para ter noção disso, desde 2006, que nós monitorizamos os números do lado criminal e, sistematicamente, os números duplicam de um ano para outro, com exceção de alguns anos. Isto é dramático, pelo que está a acontecer no mundo, mas também é dramático do ponto de vista da reação que temos de ter, porque as estruturas públicas não estão preparadas para, de um ano para o outro, terem o dobro da atividade.

Q4: Gostaria que o Pedro me falasse agora sobre o atual panorama de ciberataques em Portugal, ou seja, quais os tipos de ataques mais frequentes, os setores de atividade mais vulneráveis e os possíveis impactos destes ciberataques nas organizações.

PV: A nível mundial, temos, fundamentalmente, crimes contra dinheiro, ou seja, a generalidade dos criminosos ataca sítios que lhes possam render dinheiro. À cabeça da preocupação temos o *ransomware*. O *ransomware* é um ataque muito simples, que passa por mandar um *e-mail* para alguém, alguém dentro de uma organização abre o *e-mail* e, se for *ransomware* moderno, isto tem a potencialidade de bloquear completamente o sistema da empresa. Isto é particularmente grave com pequenas e médias empresas, porque, normalmente, não têm uma estrutura interna muito profissional de segurança, portanto ficam sem sistemas. Das duas uma, ou o gerente se lembra que, de vez em quando, tem de fazer um *backup*, ou então fica sem dados. Isto, às vezes, é economicamente dramático, porque, hoje em dia, ninguém tem papel e as faturas estão todas no computador. Não temos conhecimento que haja alguma empresa que tenha ido à falência, mas a ocorrência de um ciberataque provoca consequências sérias, porque as organizações param a atividade durante um, dois ou três dias. Em geral, as empresas, hoje em dia, têm um *backup*, pode

é já estar desatualizado. Um segundo modelo de ataque deste tipo é o chamado *CEO fraud*, ou seja, a fraude do chefe executivo da empresa. É algo que tem sido muito incisivo também com pequenas e médias empresas. É um método criminoso de crime organizado internacional, que leva alguém durante várias semanas a estudar uma empresa, ou seja, vai ao *site*, vê quem são as pessoas… Monta uma conta de correio eletrónico muito parecida com a da empresa e depois simula ser, por exemplo, o chefe do conselho de administração, que manda um *e-mail* para o diretor financeiro, às 19h00 de uma sexta-feira, a dizer que têm de fazer uma transferência imediata para a conta de um determinado cliente. A pessoa já está distraída e pode fazer a transferência, ou está alerta para esta realidade e percebe que está a ser enganado. Isto tem provocado vítimas. Nós pensamos: mas como é que alguém vai transferir 30 mil euros, 40 mil euros, 50 mil euros – normalmente, são estes os valores – para uma conta estranha sem verificar? Pois! Felizmente, a generalidade das notícias que chegam é que as pessoas foram verificar e, portanto, não aconteceu nada. Mas há muitos casos que não. E isto tem provocado prejuízos de dezenas, centenas e milhares de euros. Normalmente, as contas são em Hong Kong, na Malásia, em sítios em que é muito difícil depois investigar. Outra situação que tem provocado muito prejuízo é a dos cartões de crédito, ou seja, *sites* falsos que capturam dados de cartões de crédito ou *e-mails*, ou mensagens do *WhatsApp*, em que as pessoas são solicitadas a mandar os dados de cartão de crédito, porque o cartão ficou bloqueado. A generalidade desses cartões de crédito vão parar à *dark web*, são vendidos e a pessoa nem dá conta. Colocou os dados do cartão de crédito num *site* qualquer e não aconteceu nada, e subitamente, um mês depois, são-lhe levantadas quantias – normalmente, na ordem dos 2 mil, 3 mil, 4 mil euros – sem que se saiba de quem são. Isto é algo que provoca imensa insegurança, porque a pessoa, a certa altura, vai fazer uma compra e não sabe se deve ou não utilizar o cartão. Estas são as situações mais gravosas.

Q5: Já temos vindo a falar sobre esta questão, mas qual considera ser a importância de uma organização segura? Porquê que as organizações devem apostar na cibersegurança?

PV: A aposta na cibersegurança é essencial. Não só em Portugal, mas na generalidade do mundo, a maior parte das investigações destes ataques não são bem-sucedidas e não se descobre os *hackers*. Contudo, há muitas que têm sido bem-sucedidas e cada vez mais. Há 5 anos, por exemplo, saía uma notícia sobre este tipo de situações uma vez por mês. Neste momento, todas as semanas, há notícias de que a Polícia Judiciária conseguiu identificar redes criminosas, prendeu criminosos… Portanto, já estamos a ter uma eficácia muito maior do que tivemos no passado. Ainda assim, a eficácia é muito baixa, desde logo por duas razões, que são grandes dificuldades para ter sucesso na investigação criminal. Uma delas é o facto de sermos vítimas de criminosos estrangeiros, da mesma forma que os criminosos portugueses atacam no estrangeiro, porque sabem

que isso é muito mais seguro. Segundo, a *Internet* fornece-nos ferramentas que nos permitem sermos anónimos, isto para o bem e para o mal. Ferramentas como encriptação ou VPN's, por exemplo. Isto são ferramentas úteis e legítimas. Tal como uma arma num polícia é uma ferramenta essencial para a sua atividade, nas mãos de um bandido pode ser mortífera para a vítima. As VPN's são uma ferramenta essencial para trabalhar. Quando uma pessoa está em casa a trabalhar num assunto sigiloso, tem de usar uma VPN, para ter a garantia de que está a ligar-se à sua empresa ou à sua instituição pública com segurança. A encriptação é essencial. Para podermos utilizar o *WhatsApp*, sabendo que é uma ferramenta essencial de comunicação, temos de ter a garantia de que ninguém está a espiar as nossas conversas. Estas ferramentas que são legítimas servem aos criminosos para se manterem seguros. Portanto, esta realidade que permite aos criminosos, por um lado, atacar fora do seu país em segurança e, por outro lado, atacar com anonimato são um grande obstáculo à investigação. Muitas vezes, isto é uma barreira à nossa eficácia. Isto para lhe dizer que mais vale prevenir do que remediar, porque, de facto, remediar nem sempre conseguimos, o que quer dizer que temos de antecipar o estrago e antecipar é ter estruturas empresariais de segurança. Ter estruturas tecnológicas, ou seja, ter montado nas empresas a tecnologia de segurança necessária, entre *firewalls*, anti-*malware*, coisas dessa natureza. Por outro lado, é necessária a educação das pessoas, ou seja, sensibilização para a realidade da cibersegurança. Já lhe disse isto há bocado e insisto, cerca de 90% dos problemas de cibersegurança são problemas humanos. Ou seja, a tecnologia que as empresas e os serviços, públicos e privados, têm estava a funcionar, mas o fator humano fez a diferença. Por exemplo, o *ransomware* é um caso. O *ransomware* só funciona quando há uma pessoa a falhar, quando uma pessoa recebe o tal *e-mail* e abre sem querer. E isto só se consegue com sensibilização. Da mesma forma que é preciso ter tecnologia – porque se não tivermos tecnologia, ficamos completamente vulneráveis –, é necessário educar as pessoas nesse sentido.

Q6: O Pedro já me falou de algumas medidas e ações que as organizações devem implementar para prevenir a ocorrência de ciberataques. Quer acrescentar mais alguma?

PV: A prevenção passa pelas duas linhas que já referia anteriormente. Cada caso é um caso, portanto não se pode dizer o que cada empresa deve fazer. Mas existem duas *guidelines* que têm de estar sempre presentes. Primeiro, ter em conta a tecnologia e implementar medidas tecnológicas de segurança. Segundo, apostar na formação específica das pessoas, ou seja, sensibilização das pessoas para as questões da cibersegurança. E isso é um trabalho recorrente, em ciclos, porque aquilo que está a acontecer hoje em dia não é aquilo que acontecia há 5 anos. Há 5 anos havia problemas que hoje já não temos, até porque a tecnologia veio resolver. Por exemplo, receber meramente vírus por correio eletrónico quase já não acontece, porque os antivírus liquidaram isso.

Portanto, sensibilizar as pessoas para o que está a acontecer tem de ser uma atividade recorrente. Da mesma forma que, por exemplo, as pessoas nas empresas têm, de vez em quando, formações de inglês, ou formação em práticas de segurança no trabalho. Portanto, estas duas linhas de força são as linhas essenciais.

Q7: Por último, qual considera ser o futuro dos ciberataques em Portugal?

PV: O cibercrime, neste momento, é uma indústria, portanto quem se dedica ao cibercrime é o mesmo tipo de pessoas que se dedica ao tráfico de droga ou ao tráfico de pessoas ou outro tipo de negócio ilegal, como o tráfico de armas. Portanto, o cibercrime é mais uma área de negócio criminosa e que tem a seu favor o facto de a digitalização não ter parado, porque cada vez há mais vida digital e não se prevê que pare. Quer dizer, não é por todos já termos telemóvel, que parou a progressão, porque cada vez há mais serviços no telemóvel, mais entidades que vendem coisas na *Internet*, mais serviços públicos que estão na *Internet*. E não se vê que haja um momento em que a curva pare. Continua a haver cada vez mais digitalização e, enquanto houver digitalização, continua a crescer o número de pessoas que quer ganhar dinheiro à custa destas atividades. Portanto, quanto mais pessoas houver a circular nas redes, mais serviços digitais há, mais dispositivos há, portanto mais incidentes podem potencialmente ocorrer. A não ser que nós tenhamos uma atitude preventiva de educação das pessoas, no sentido de as levar a cumprir as regras, a ser cautelosos… Então aí diminui, ou potencialmente diminui. Por isso digo que o futuro é risonho. Quais são os incidentes? Não sei…

Apêndice 7: Entrevista Duarte Freitas

Q1: Gostaria que o Duarte começasse por me falar um pouco sobre a sua experiência na área da Cibersegurança.

Duarte Freitas (DF): Eu comecei a trabalhar em segurança nos anos 90. Na altura, o conceito de cibersegurança ainda não existia, mas comecei com a primeira necessidade de algumas organizações se protegerem através de *firewalls*, uma vez que se começaram a ligar à *Internet*. Portanto, é no final dos anos 90 que se começam a criar as primeiras ligações à *Internet*. Então, já havia uma sensação de que era preciso criar regras, haver políticas de segurança mínimas para que as organizações ficassem protegidas. Estive sempre ligado muito à segurança e a soluções de valor acrescentado, quer seja na proteção, quer seja na análise de eventos, blogs… Depois tive no Grupo Sonae, onde estive muito ligado ao comércio de soluções, portanto, de tecnologia. Depois, a Sonae comprou uma empresa que era dos maiores *players* de segurança na Península Ibérica – e até na Europa –, completamente dedicado a cibersegurança. Isso já foi nos anos 2000 e já havia uma

definição muito concreta do que seriam os serviços e que maioria de serviços as organizações iriam necessitar. Chamava-se S21Sec, estive por lá e depois fui convidado para ir para um fabricante, a Fortinet, que é um fabricante de *firewalls* e outras ferramentas de segurança. Depois, vim para a IBM, onde estou em *Security Services*, desde 2021, e estou muito focado em serviço. Neste momento, já não olho só para a tecnologia. A tecnologia é um meio, mas são os serviços que gravitam à volta da cibersegurança que eu estou focado e que nós prestamos. Devido ao ano 2022 que tivemos, o nosso serviço-estrela foi a resposta a incidentes, portanto respondemos a muitos incidentes. Ajudámos organizações a recuperar de grandes incidentes. Depois temos tudo o que é serviços de *security assessment*, temos tudo o que é os *penetration tests*… A nossa oferta está muito organizada à volta do que é o *framework* NIST, *zero trust* e por aí adiante.

Q2: Já que me falou de aconselhamento às organizações, a IBM também ajuda as organizações a responder ao incidente do ponto de vista comunicacional?

DF: Quando existe um incidente, articulamos com os gabinetes de crise e somos uma fonte de informação bastante útil para os gabinetes de comunicação. Temos as nossas teorias e boas práticas dentro daquilo que é a comunicação, portanto acabamos por aconselhar naquilo que é a resposta ao incidente. Mas claramente gostamos de fazer um trabalho a montante. Quando ajudamos os nossos clientes a prepararem-se para evitarem que um incidente grave aconteça, ajudamos e aconselhamos também como deve ser a comunicação. Mas não assumimos, nunca, o papel de ser o comunicador e de produzir os conteúdos para aquilo que será a comunicação final com a imprensa ou com quem quer que seja.

Q3: Então começamos já por abordar este tópico. Que medidas e ações de comunicação considera que as organizações devem implementar na resposta a um incidente de cibersegurança?

DF: Se, por um lado, eu acho que é muito importante comunicar-se rápido e de forma clara, por outro lado, acho que tem de haver alguma contenção, tem de se perceber bem qual é o impacto que o incidente está a ter na organização e, inclusive, nos seus clientes, nos seus colaboradores, em todas as pessoas que estão associadas e organizações terceiras que se relacionam com a empresa atacada. Depois disso, o mais importante é tranquilizar quem acha que pode ter dados ou informação em risco. Essas pessoas devem ser informadas de forma clara sobre aquilo que está a acontecer. Se vai haver disrupção nos serviços, se há informação privada que pode ser comprometida também devem ser informados… Relativamente ao detalhe e à origem, tem de se ter muito cuidado com aquilo que se divulga, até porque, muitas vezes, não sabemos quem é que executou esse ataque e até podemos estar a dar informação a pessoas ou entidades que estão

envolvidas no próprio ataque. Portanto, também é preciso perceber muito bem a quem é que vamos divulgar essa informação. Por exemplo, nós tivemos envolvidos na recuperação de um incidente, em que uma das críticas que foi feita à organização – era uma organização bastante grande, em que houve algum mediatismo à volta desse ataque – foi o facto de estarem muito tempo em silêncio. Portanto, eles comunicaram que tinha havido um ataque, mas depois não deram muito mais detalhes. E percebemos que também tinha a ver com a própria natureza do ataque e das entidades envolvidas. Havia muitas entidades que, se calhar, havia uma necessidade de comunicar mais detalhes sobre o ataque, mas havia uma delas, por exemplo, que fazia parte do problema e não da solução. Portanto, essa entidade estava envolvida no próprio ataque e convinha que eles não divulgassem essa informação, de forma que a investigação decorresse normalmente e nós pudéssemos recolher todos os elementos que nos levassem a tirar as conclusões certas ou que houvesse contágio ou alguma tentativa de esconder ou disfarçar aquilo que tinha acontecido. Portanto, eu acho que a comunicação deve ser de forma faseada. À medida que vamos eliminando tudo aquilo que nos pode prejudicar, eu acho que deve ser divulgado o máximo de informação. Até acho que deve haver dois tipos de comunicação. Uma comunicação entre todas as organizações que estão à volta, que são pares. Nós fizemos questão de passar informação a empresas que estavam no mesmo setor de negócio com quem a IBM, por exemplo, também tinha relação, com autorização, é claro, deste grande grupo. Mas criámos, então, um fórum onde pudemos partilhar os nossos problemas, os nossos desafios, alguns factos que estavam a ocorrer, que permitiu também às próprias organizações tomarem medidas preventivas… Fomos descobrindo qual é que era o vetor de ataque, como é que tinha sido feita a execução do próprio ataque. Então, partilhámos toda a informação que evitasse que outras organizações semelhantes pudessem ser atacadas. Essa comunicação eu acho que deve ser imediata, até para tentar perceber se no mesmo setor de negócio, por exemplo, houve ataques semelhantes. Além de partilhar, "beber" de toda a informação disponível que outras organizações podem ter. Portanto, este é o primeiro tipo de comunicação. Depois com o público em geral, é importante informar sobre o que está a acontecer, ou seja, eu acho que toda a informação que não prejudique uma investigação ou a recuperação, eu acho que deve ser divulgada. Não há que ter medos. Há um chavão muito grande, que já deve ter ouvido falar em cibersegurança que é: todos vamos ser atacados, não sabemos é quando. E é preciso acreditar mesmo nisto. Eu nunca critiquei nenhuma organização que tivesse sido atacada, porque, muitas vezes, desconheço as razões pelas quais foram atacadas, mas eu sei que, por muito esforço que todos nós façamos para nos proteger, quem está do lá de lá a atacar está sempre à frente, está sempre um passo adiante. O esforço e o investimento que eles fazem é 10 vezes superior quase àquele que nós temos capacidade de fazer a nível de proteção. Por isso, não há que esconder, acho que a comunicação deve ser muito transparente, filtrando apenas aquilo que pode prejudicar a

investigação ou que pode pôr em causa a reputação. E falando de reputação da organização, já há casos – há um muito conhecido, que foi o da Vodafone – onde a comunicação transparente e contínua foi crítica para que a reputação fosse muito menos afetada. O ataque da Vodafone teve um grande impacto nos clientes e nas empresas – que também são clientes – e foi minimizada, porque houve uma comunicação muito direta, muito frontal, muito transparente com todas as entidades. Por isso, eu acho que há claramente ganhos com esta comunicação direta, como lhe estou a dizer, salvaguardando sempre toda a informação que não seja importante divulgar e que seja importante conservar para nós, para podermos prosseguir com a investigação.

Q4: Agora, gostaria que o Duarte me falasse um pouco sobre a evolução dos ciberataques em Portugal.

DF: Nós produzimos, anualmente, dois relatórios. Um chama-se *Cost of a Data Breach*, que tem que ver com o custo de uma fuga de informação. O outro chama-se *IBM Security X-Force Threat*. E nesse *IBM Security X-Force Threat* há uma curiosidade muito grande. Portugal, pela primeira vez, teve um capítulo dedicado a si. Isto porquê? Porque na Europa nós fomos o terceiro país mais atacado em 2022. Por isso, em termos de magnitude, nós ainda não conseguimos – nem o nosso departamento de investigação consegue – atribuir uma justificação segura, que nós diríamos: "esta é a razão pela qual Portugal foi tão atacado". Aquilo que nós sabemos é que começou no dia 1 de janeiro, com um grande ataque a um grupo de *media* e não parou. Pela quantidade de sistemas atacados e por serem muito parecidos uns com os outros, entendemos que foi descoberta uma vulnerabilidade, que alguém iniciou um ataque e divulgou que tinham feito um ataque bem-sucedido a um determinado sistema – que tem uma série de vulnerabilidades – e, a partir daí, vulgarizou-se. Isto é, houve uma série de organizações que agarraram nessa informação que estava na *dark web* de que Portugal tinha uma série de sistemas com vulnerabilidades e começaram a ocorrer com muita frequência. Deixe-me dizer-lhe que tudo o que foi sistemas de *cloud* foram tipicamente alvos para este tipo de ataques em 2022. Aliás, *cloud* ou virtualização, em que um dos sistemas mais conhecidos é o *VMware* e foi bastante atacado. O que eu lhe posso dizer é que quase todos os grupos atacantes mais conhecidos estiveram a atuar em Portugal, quer seja na banca, quer seja no retalho, quer seja nas telecomunicações… Houve muitos ataques. E não foi só. Houve claramente um foco nas grandes empresas, não há dúvida, mas também houve muitas PMEs. E quando falo de PMEs refiro-me às imediatamente abaixo das grandes empresas. Tentando dividir o que são PMEs, existem PMEs que são mesmo pequenas, existem médias e depois existem PMEs grandes. E eu acho que as PMEs grandes foram muito atacadas. Na área, também, da saúde, dos serviços, como educação, gabinetes de advogados… Houve muitos ataques a esse tipo de organizações. O que também lhe posso dizer é que a maioria não foi divulgada e houve muitos que

pagaram. Atenção que o que lhe vou dizer agora é uma opinião do Duarte Freitas e não uma posição que a IBM consiga transmitir relativamente aos resgates que foram pagos. Aquilo que eu sei, pelo conhecimento que fui tendo, é que houve muitas pequenas e médias empresas a pagar o resgate. Porquê? Porque perceberam que não tinham tomado medidas preventivas e, então, o custo de tentarem recuperar sem pagar era muito superior àquilo que lhes estava a ser pedido, especialmente depois de entrarem em processos de negociação. Deixe-lhe dizer, também, que a IMB não recomenda pagamentos de resgate, nós não assumimos papéis de negociadores. Existe já uma série de entidades na área da cibersegurança que assumem esse papel de tentar negociar um valor mais aceitável. Isto tudo em caso de *ransomware*, claro. Aquilo que realmente assistimos é que houve muitas entidades a pagar porque não tinham tomado medidas que lhes permitisse depois recuperar de forma mais tranquila ou controlada de um ataque de *ransomware*. A verdade é que houve muito *ransomware*, com dois sentidos. *Ransomware* para pedir apenas o dinheiro do resgate, portanto um dos objetivos era pagar para obter a chave de desencriptação. Mas também houve muito apoderar-se de informação. Eles não só encriptavam os dados, mas apoderavam-se dessa informação. E o facto de terem em seu poder informação confidencial também utilizavam como argumento para pedir o resgate. Houve muitas organizações que, por exemplo, achavam desproporcional o valor que lhes estava a ser pedido em questões de resgate e depois percebiam que eles tinham acedido a informação que era de tal maneira valiosa que pediam valores exorbitantes. E muitas organizações só perceberam que lhes estavam a pedir aquela quantia porque eles tinham em seu poder informação que não podia ser divulgada. Há dois vetores de ataque. Um que são vulnerabilidades de plataformas virtuais que foram exploradas. Muita falta de *patching* em sistemas. E depois o vetor tradicional, o *phishing*, através do *e-mail*. O utilizador continua a ser um dos elos mais fracos. Mas houve muitos ataques a sistemas por falta de *patch*, por falta de estarem atualizados. Também houve uma alteração curiosa do *ranking*. Quem liderava o *ranking* das entidades atacadas era banca e seguros e, pela primeira vez, em 2021, quem assumiu a liderança nesse ranking foi o setor industrial. E há uma explicação para isso. O sistema industrial era aquele que estava menos evoluído, era aquele que menos estava ligado à *Internet*, que não estava *online*. Era equipamentos antigos, linhas de produção de fábricas, por exemplo… Se olharmos para uma fábrica há 5 anos, poucas tinham ainda arquiteturas que lhes permitissem estar ligadas à *Internet*. Existe agora um processo de transformação digital muito específico no setor industrial, que tem que ver com a convergência do IT e do OT. Essa convergência permitiu que equipamentos antigos, sistemas antigos – esses sim, com muita falta de atualização – fossem muito atacados e, à medida que foram sendo descobertos, claramente houve um foco no ataque a esses sistemas. É surpreendente e curioso vermos que as entidades financeiras, que é onde está o dinheiro e onde normalmente se consegue pedir resgates mais elevados, deixaram de ser o foco dos

atacantes. Segundo o nosso relatório *Cost of a Data Breach*, uma das coisas que continua realmente a crescer exponencialmente é o custo de um incidente. Apesar de as organizações estarem a investir cada vez mais na proteção, mesmo assim o custo continua a aumentar exponencialmente.

Q5: Considera, então, que houve uma clara evolução daquilo que é a magnitude e o impacto dos ciberataques em Portugal ao longo dos anos?

DF: Sim, sem dúvida. Portugal andou fora do radar durante uma série de anos. Eu em 2011/2012 andava a pregar e tinha dificuldade em alertar alguém para esta problemática. Porquê? Porque Portugal não aparecia no radar… Independentemente até da sofisticação, dos ataques estarem a evoluir, não havia uma sensação de alarme, ninguém temia ser atacado. Eu acho que 2016, em PMEs, foi quando eu comecei a ver mais ataques. Eu considero um marco, porque nunca tinha sido chamado para responder a tantos incidentes e achei interessante, porque era a pequenas e médias empresas, *ransomware* já… A primeira onda de *ransomware* que eu me lembro foi em 2015/2016, onde em pequenas empresas lhes era pedido até pouco dinheiro. Era *easy money*. O objetivo era que pagassem. E lembro-me de muitas organizações serem atacadas uma vez, pagarem, voltarem a ser atacadas duas semanas depois, pagarem outra vez e só à terceira é que chamavam uma entidade que lhes dissesse "eu não vou abrir mais as minhas comunicações até ter um plano estratégico de segurança que evite que isto aconteça outra vez". Eu acho que entre 2020 e 2022, assistimos a um crescimento progressivo, isto é, técnicas muito mais evoluídas… Por exemplo, no *spear-phishing* vi coisas que nunca tinha visto naquele ataque mais dedicado a papéis estratégicos dentro das organizações. Foi a primeira vez que eu comecei a ver que havia muito investimento por parte do atacante neste tipo de ataque. E em termos de quantidade de persistência, claramente também aumentou. Aquilo que temos noção é que os ataques que eram normalmente feitos por autodidatas, por comunidades de estudantes que gostariam de desafiar o *status* e exibir os seus troféus, em que o dinheiro não era a motivação principal, claramente evoluiu bastante para que o dinheiro passasse a ser a principal motivação. Esses autodidatas, que antigamente exibiam os seus troféus, quase que se retiraram, porque têm receio de ser confundidos com este ciberterrorismo, com este cibercrime organizado.

Q6: O Duarte apontou-me já algumas razões para este aumento de ciberataques. Quer acrescentar mais algum fator que tenha motivado o aumento de ciberataques em Portugal, desde sensivelmente 2020?

DF: Claramente que não se pode deixar passar a transição digital a que todos nós fomos obrigados nestes últimos anos. Como é óbvio, houve uma migração de muitos sistemas para a *cloud* e depois o facto da conetividade passar a ser feita a partir das nossas casas. Houve sistemas que tiveram

que publicar aplicações para o exterior, que antigamente não eram necessárias… Claramente esta transição digital foi um grande gatilho para que aumentasse os ciberataques durante a pandemia. O que eu acho foi que o tipo de ataque que ocorreu durante a pandemia foi, mesmo assim, diferente daquele que nós viemos a sentir, em Portugal, em 2022. Quando foi a pandemia e todos viemos para casa, houve algum alarmismo do lado das organizações que se estavam a proteger, isto é, até houve investimento adicional em proteger alguns sistemas e aplicações que passaram agora para a *cloud* e que estavam expostas e publicadas na *Internet*. A partir do momento em que houve um regresso à normalidade e as empresas se esqueceram que foram forçadas a fazer algumas transformações, mas que não olharam para alguns detalhes, por exemplo, de algumas aplicações, é que houve aqui um aliviar da vigilância para esses sistemas… Portanto, eu acho que a pandemia claramente ajudou para este aumento, mas refletiu-se um ano e meio quase depois, sobretudo em 2022.

Q7: Atualmente, qual considera ser o grau de preparação das empresas portuguesas em cibersegurança?

DF: Se olharmos para o *ranking* das organizações, em que o setor industrial passou para a liderança e ultrapassou o setor financeiro, há duas razões. A primeira é o facto de se ter descoberto a convergência do IT com o OT e, por isso, há mais vulnerabilidades nestas organizações. Mas o setor financeiro fez, claramente, grandes investimentos e, por isso, também se vê que, apesar de aumentar de ano para ano, o setor financeiro aumentou menos do que aquilo que estava a aumentar. Portanto, eu acho que há consciência. Do ponto de vista de *awareness*, tem havido um aumento crescente nas organizações. A questão continua a ser a dificuldade dos *chief information security officers* justificarem os grandes investimentos que têm de ser feitos aos seus departamentos financeiros, aos seus CEOs… Por exemplo, nós estamos a dar muita importância à quantificação do risco. Eu vou-lhe dizer que uma das organizações que nós ajudámos a recuperar o ano passado, quando foi atacada, tinha previsto um determinado tipo de investimento e, quando nós lhe dissemos que a iríamos ajudar, mas que isso teria um custo, eles não tinham noção de quanto iriam perder por dia caso o negócio deles tivesse parado. E ao fim de dois ou três dias, a partir do momento em que perceberam qual era o impacto no negócio, disseram-nos: "por favor, avancem, porque cada dia que estamos parados equivale a cinco ou dez adjudicações que nós vos fazemos para nos ajudarem a recuperar". Por isso, eu acho que ainda há uma dificuldade muito grande dos departamentos de cibersegurança se justificarem junto das suas organizações o porquê de terem de fazer alguns investimentos. Às vezes são grandes, mas comparado com o impacto que isso pode ter afinal não são nada. Mas claramente há um aumento de consciência. Eu tenho receio é que não se continue a investir aquilo que é necessário, que se continue a fazer gestão de tesouraria

relativamente a um tema tão importante. A sensação que nós temos é: "eu antigamente não tinha noção do risco a que estava exposto, agora já sei". A maioria das organizações não quantifica o risco, mas tem noção dele, qualifica. E eu acho que há muitas organizações que ficam com a sensação falsa de que estão mais seguras agora que o conhecem. Porquê? Porque tomam algumas medidas e assumem o risco, porque o conhecem. O problema é que existem muitas alterações nas organizações e o risco muda, está sempre em evolução. Por isso, eu acho que continua a ser um nível muito fraco. Nota-se uma melhoria, mas continua a ser fraco. Se tivesse de colocar numa escola de 1 a 10, diria que o grau de preparação é entre um 4,5 e um 5. Saiu de muito fraco para um médio fraco. E não é só no investimento tecnológico, isto passa muito por conhecer, por visibilidade, por ter capacidade de agir, por proteger realmente aquilo que interessa. Existe esta filosofia do *zero trust network*, já ouviu falar de certeza. Apesar de ser um tema bastante batido, continua a ser algo que as empresas devem investir. Devem olhar para esse conceito e tentar segui-lo. Dentro das várias etapas que estão compreendidas naquilo que é uma estratégia *zero trust*, as organizações devem olhar para elas de forma muito séria e desenhar planos estratégicos que lhes permitam ir fechando capítulos e etapas desse *zero trust network*. Como digo, há muitas organizações que acham que por fazerem determinados tipos de investimentos, por exemplo, em tecnologia… Às vezes, vejo organizações gastarem dinheiro em tecnologia e vão pondo camadas de segurança umas em cima das outras, mas não percebem porque é que o estão a fazer e, às vezes, essa sobreposição de camadas de segurança não as torna mais seguras. Portanto, eu acho que compreender o porquê das coisas, definir um plano estratégico a médio-longo prazo, ter consciência do nível de maturidade em que estou e perceber para onde é que eu quero ir e justificar muito bem à minha administração que tenho de fazer estes investimentos. Uma das mensagens mais importantes que eu tenho é: quantifiquem o risco. Se convertermos isto para uma linguagem universal, que é o dólar e o euro, é muito mais fácil comunicarmos internamente com toda a nossa administração e dizer-lhes: "isto é a probabilidade de um incidente ocorrer e este é o impacto financeiro que vai ter". Eu acho que é muito mais fácil um *chief information security officer* suportar a razão pela qual temos de fazer este investimento e temos de ter um plano estratégico, que tem de ser cumprido rigorosamente. Por isso, respondendo à sua pergunta mais uma vez, o nível ainda é medíocre, mas claro que está a evoluir.

Q8: O Duarte falou-me agora, essencialmente, de um fator técnico, mas também temos o fator humano, que são os colaboradores. Considera que as organizações devem apostar na formação dos seus colaboradores para melhor se protegerem face à ocorrência de um ciberataque?

DF: Sim, sem dúvida. Como já lhe disse anteriormente, o utilizador continua a ser o elo mais fraco e continua enquanto não dermos formação de tal maneira que já seja automático, como travar num carro quando vemos o trânsito parado, como trancar a porta quando saímos de casa… Mas a formação tem de ser feita de forma interessante. Um dos investimentos que as organizações têm de fazer – e até o nosso papel como IBM – é tornar as formações interessantes, desejáveis, para que os colaboradores desejem ter mais formações do género, porque acrescentam valor, porque se sentem mais seguros e sentem que estão a tornar a organização mais segura. Essa sensação de valor tem de ser cada vez mais bem passada para o colaborador. E também devem fazer outro tipo de formação ou de *awareness* que é exemplos e demonstrações ao vivo – e nós na IBM fazemo-lo – do impacto que isto tem numa organização. Por exemplo, uma das coisas que fizemos foi chamar uma equipa de *ethical hackers* que vão às empresas e demonstram um ataque, que pode ser num sistema criado de propósito, mas que é uma réplica dessa organização. Portanto, imagine nós criarmos uma réplica da sua empresa e simulamos qual é o impacto que pode ter um ataque, a facilidade e a rapidez com que podemos fazer um ataque. E depois um auditório ter grande parte dos colaboradores a exclamar como foi fácil por causa de uma ação simples de clicar num *link* que era de confiança, que até foi colocado de propósito na *Intranet* da organização, e a facilidade com que nos apoderámos de alguns sistemas, eu acho que é muito importante. E envolvê-los na testagem… Há muitas organizações com planos estratégicos, que fizeram *security assessments, gap analysis*… fizeram muitas análises e tiveram muitas avaliações. E até têm planos e testam-nos com frequência. Eu vou-lhe dizer, grande parte das organizações que foram atacadas tinham planos de segurança, tinham uma maturidade acima da média… Mas nunca testaram os planos de resposta. Portanto, envolver também os colaboradores, os utilizadores, na parte da testagem, para eles terem consciência de que têm um papel a desempenhar na proteção da organização. Por isso, sim *awareness*, sim formação, mas formação não só sobre o que é a ameaça, mas como é que eles podem fazer parte da solução. Transmitir-lhes mesmo que eles são uma peça fundamental na prevenção, mas também podem ter um papel muito importante na própria recuperação do incidente.

Q9: Já me foi indicando algumas medidas e ações que as organizações devem implementar para prevenir a ocorrência de ciberataques. Quer acrescentar mais alguma?

DF: Eu já lhe falei em tudo o que seja realmente avaliações… Avaliação do risco, definição de planos estratégicos, sobretudo de um plano estratégico de segurança a médio-longo prazo, ter uma equipa que o acompanhe, que consiga atualizá-lo, que consiga testá-lo com frequência. Depois, eu considero importante ter linhas orientadoras, sendo a estratégia do *zero trust* muito importante e uma referência. Mas claramente, investir na gestão de identidades e acessos, gestão privilegiada de acessos… Olhar muito para a rede convencional, olhar para sistemas que parece que estão protegidos por natureza e avaliá-los. Mas digo-lhe, gestão de identidades e acessos e gestão privilegiada de acessos é mesmo muito importante. Isto é uma componente muito importante do *zero trust* e vou-lhe dizer que, em muitos dos ataques a que respondemos o ano passado, um dos problemas foi que, ao apoderarem-se do sistema, conseguiram muito facilmente escalar privilégios de utilizadores. Isto tinha que ver com privilégios mal atribuídos, com ausência de múltiplo fator de autenticação… Muito importante, por exemplo, a questão de identificar quais são todas as aplicações que podem ser críticas e que podem estar expostas a ataques e aplicar-lhes múltiplo fator de autenticação. Vou reforçar novamente a questão da testagem, porque aquilo que estamos a ver é um aumento significativo do investimento em análise, em avaliações do ponto de vista de qual é a postura da organização face a ameaças, mas depois não se atualiza e não se testa… Existe, ainda, um outro domínio que tem que ver com sistemas, com infraestruturas, com planos de recuperação, como o *disaster recovery plan*, por exemplo, ou o *business continuity plan*. Cada vez mais estes dois planos têm de estar em harmonia com aquilo que são as ciberameaças hoje em dia. Portanto, eles têm de trabalhar em conjunto e têm de ser atualizados. Se no passado, antes da componente ciber ser tão importante, ter um plano de recuperação de negócio já era importante estar atualizado, agora ainda mais. A velocidade com que a ciberameaça evolui é muito superior a outro tipo de desastres. Portanto, testar e manter atualizado é realmente fundamental.

Q10: Quais considera ser as principais tendências e desafios com impacto na área da cibersegurança?

DF: Neste momento, estamos preocupados e temos feito cada vez mais ações de consciencialização dos nossos clientes em termos de Inteligência Artificial, que pode ser realmente uma ameaça. Por isso, fazer avaliações de qual é a nossa exposição a tecnologias baseadas em Inteligência Artificial começa a ser cada vez mais importante. E depois a IBM é pioneira na computação quântica e, neste momento, também estamos muito preocupados com o impacto que a computação quântica poderá ter, por exemplo, nas chaves criptográficas. Nós sabemos que, hoje em dia, há chaves criptográficas que poderão demorar 5 mil anos a ser decifradas, mas com o

aumento da capacidade de processamento dos cúbitos da computação quântica possa ser reduzido para 3 ou 4 dias. Portanto, este é um tema que está a começar a preocupar algumas entidades, sendo as entidades financeiras aquelas que estão mais preocupadas com esta questão. É, sobretudo, uma tendência de futuro, é olhar para as chaves criptográficas e cifras que estamos a utilizar e pensar qual será o impacto da computação quântica. Quanto à IA, é uma loucura. Já lhe disse o que é possível fazer de forma simples, mas também é uma loucura, porque vai começar uma corrida do gato e do rato. Por um lado, estão os *hackers* a procurar utilizar a Inteligência Artificial para atacar e, do nosso lado, é também uma corrida louca para tirar proveito daquilo que a IA nos pode dar para proteger. Em termos de tendências atuais, o que temos vindo a assistir é que as principais entidades atacantes analisam os diversos *malwares* e as diversas técnicas que têm utilizado e estão a reinventar-se através daquilo que cada técnica tem de melhor. Imagine, existe agora um *malware*, que não me recordo do nome, cuja última versão é o reaproveitamento do que há de melhor em três ou quatros *malwares* diferentes, que nem sequer são da mesma família. Deixe-me dizer-lhe também uma grande evolução nos ataques que diz respeito à velocidade com que eles conseguem tornar um ataque eficaz. Isto é, muitas vezes, chegávamos a estar 240 e poucos dias desde o primeiro contacto até que o atacante conseguisse ser eficaz. Hoje em dia, pode ser realizado facilmente em 72 horas. Portanto, essa é uma das grandes transformações e a tendência mais atual. Quanto à sofisticação, é o que lhe estava a dizer, já tem muito que ver com reaproveitar o que há de melhor em cada técnica.

Q11: Por último, qual considera ser o futuro dos ciberataques, sobretudo em Portugal?

DF: Eu acho que pode haver uma tendência para que o ciberterrorismo e o cibercrime andem mais próximos. Portanto, considero que o resgaste que se vai pedir para possíveis impactos em infraestruturas críticas será muito elevado. Eu acho que o futuro do ciberataque é dar-lhe, pelo menos, uma dimensão e uma sensação de ameaça tão grande que os próprios Estados vão começar a pensar que vão estar sob ameaça. Pode ser mesmo muito catastrófico. Eu não tenho dúvida de que os ciberataques já são eficazes, mas acho que uma das tendências que realmente vai aumentar é tentar transformar essa ameaça em algo que pode ser catastrófico e que os Estados e as organizações tenham mais receio e estejam dispostas, em situações críticas, a pagar mais para evitar um impacto na organização. Já lhe falei da computação quântica e acho que poderá ser um instrumento para aumentar essa sensação de ameaça. Vai passar, também, pela Inteligência Artificial. Eu acho que nós ainda estamos muito verdes na prática, mas do ponto de vista da teoria já há muito trabalho a ser feito. Nós ainda só estamos a olhar para o facto de o ataque, utilizando a Inteligência Artificial, seja o típico que vem do exterior e não pensamos que podem ser ameaças internas de forma muito simples e eficaz. Há aqui um terceiro pilar que eu normalmente abordo e

estou-me a esquecer completamente… Mas posso referir também a *Internet of Things*, que claramente vai massificar e tornar-se um risco. Na verdade, a IoT já faz parte do presente, só que ainda não se massificou. Acho que a partir do momento em que se massificar, vai trazer riscos acrescidos às organizações.

Q12: Penso que abordamos todos os tópicos que estavam previstos inicialmente. Não sei se o Duarte quer acrescentar mais alguma ideia que considere pertinente e que não tenhamos abordado.

DF: Relacionado com a comunicação, eu acho que não lhe falei na importância que é definir um gabinete de crise, na gestão de crise, em caso de incidentes ciber. Mas é muito importante ter todos os departamentos envolvidos, desde o legal, recursos humanos, claramente comunicação… E também treinar bem o departamento de comunicação para o que fazer e como responder a um incidente.

Apêndice 8: Entrevista Alexandra Abreu Loureiro

Q1: Gostaria que a Alexandra começasse por me falar um pouco sobre a sua experiência na área da Comunicação.

Alexandra Abreu Loureiro (AL): O *Brunswick Group* é um grupo de aconselhamento reputacional a empresas geralmente cotadas e, portanto, aos CEO's em particular. Aconselhamos em situações de comunicação críticas. Pode envolver tudo o que sejam questões reputacionais, como, por exemplo, relações com os *media*, relações com os vários *stakeholders*, relações institucionais, comunicação da narrativa quando tudo está bem e quando tudo está errado. Ou seja, quando há uma fusão ou uma aquisição, deve-se comunicar aos analistas, aos *stakeholders* que vão desde o público em geral ao público em particular. Numa situação de crise, por exemplo, um incidente *cyber*, aconselhamos como a empresa deve fazer, como fazer, a quem fazer, como falar aos seus *stakeholders*. São dois exemplos da forma como costumamos agir como empresa de comunicação reputacional. Somos a empresa número um em Inglaterra e nos Estados Unidos, somos uma das maiores empresas mundiais neste campo de aconselhamento crítico comunicacional e reputacional. Eu represento e dirijo as operações da firma para os países de língua portuguesa, sou *partner* em Londres, sou oficial em Portugal. Relativamente à minha experiência anterior, fui jornalista durante muitos anos. Grande parte da minha carreira foi como jornalista de política internacional e foi, também, como pivô. Comecei a minha carreira num jornal americano, o *International Herald Tribune*, fiz vários estágios televisivos na CNN, trabalhei na *BBC World Service*. Em Portugal, lancei a SIC Notícias e, portanto, tenho uma experiência de jornalismo

importante, na medida em que nos dá a primeira perspetiva da comunicação, que são os *media*. Segunda perspetiva, trabalhei no governo, fui assessora do Ministro da Defesa, fui assessora do Ministro dos Negócios Estrangeiros e, portanto, trabalhei para o segundo pilar da comunicação que é a parte governamental. A junção da minha experiência nos *media*, por um lado, como jornalista, repórter e apresentadora, assim como assessora de dois governos resulta no terceiro pilar da comunicação que é a comunicação empresarial – é efetivamente o que fiz nos últimos 12 anos. Portanto, foi desenvolver a prática e desenvolver o *Brunswick Group*, que não estava presente em Portugal e em países de língua portuguesa.

Q2: Comecemos, então, com a parte da comunicação de crise em cibersegurança. Qual considera ser a importância da comunicação de crise numa situação de ciberataque? Ou seja, numa empresa, o que assegura e o que previne, tanto a nível interno, como a nível externo?

AL: Acho que os últimos 5 a 7 anos foram decisivos. Se voltássemos atrás a 2016 ou 2017, a maior parte das empresas achava que ciber era uma questão que estava no domínio do IT. Portanto, era uma questão meramente interna ou meramente técnica. Nos últimos 5 a 7 anos, o público percebeu que isto não era o caso… Qualquer um de nós que tenha uma conta num banco, uma conta numa linha aérea, uma conta de telefone, sabe perfeitamente que a cibersegurança é o pão nosso de cada dia. Não há nenhuma plataforma de nenhuma empresa que não deva e que não possa, hoje em dia, investir absolutamente na sua segurança cibernética. É como ter uma chave à porta de casa. Há 50 anos, as pessoas podiam sair de casa e deixar a chave na porta, hoje em dia ninguém o faz. A cibersegurança é igual, só que os prazos são mais curtos. Há 5 anos, se calhar ninguém se lembrava de fechar a chave do computador, ou seja, fechar efetivamente o computador, pensar duas vezes antes de clicar num *link*, pensar três vezes antes de abrir um vídeo ou um ficheiro. Hoje em dia, acho que toda a gente já pensa, pelo menos, uma vez em todas estas questões. Portanto, o paralelo da chave e da cibersegurança é muito importante. O que uma empresa faz na eventualidade de um ataque ciber também, provavelmente há 5 anos, não estava nos planos de crise e atualmente é número um. Aquilo que era visto como uma operação técnica, hoje em dia é visto como um absoluto requisito de liderança. Quando uma empresa é afetada – e tivemos várias nos últimos anos no panorama das telecomunicações, operadoras, serviços profissionais, bancos –, o primeiro passo é vir a público e confirmar que efetivamente aconteceu, explicar o que aconteceu, é comunicar absolutamente em tempo real com os seus *stakeholders*. Podem ser pacientes, podem ser clientes… houve até vários exemplos na área da saúde. O que é importante é, número 1: reconhecer o que aconteceu, comunicar o que está a acontecer – vou relembrar aqui que estas coisas acontecem em tempo real e, portanto, podem mudar de hora a hora – e, muitíssimo importante, a etapa de liderança. Portanto, se existe uma etapa de preparação e de liderança, existe

uma terceira etapa que é *recover*. Portanto, *prepare, lead and recover*. Eu diria que, para mim, este é o triângulo. Preparar significa que as empresas têm de estar preparadas com simulações deste tipo de situações, não só ciber, mas de qualquer tipo de crise. Liderar é porque, no momento em que acontece, o CEO vai ter de continuar a gerir e a gerar negócio, enquanto a equipa está destinada, preparada e treinada – e, se não está, chama as pessoas certas para isso. Em terceiro ponto, *recover* ou recuperação dessa situação é absolutamente chave para a segurança da relação com um cliente. Uma empresa só pode continuar se as pessoas acreditarem nela. *Breach* pode acontecer a todos. O que é decisivo é a forma como uma empresa lida com isso, comunica em tempo real, factual e de forma transparente com os seus *stakeholders* o que está a acontecer. A atualização dos dados é muito importante, ir atualizando, explicar o que aconteceu, quais são os atos e os instintos que a empresa tem para reagir a este tipo de segurança. E depois, o que pretende fazer para recuperar a segurança das pessoas e dos clientes.

Q3: Sendo assim, qual considera ser o papel do profissional de Relações Públicas de uma organização numa situação de ciberataque?

AL: Número um, esse profissional tem de existir numa empresa, caso a empresa ainda não tenha. As que têm, têm de profissionalizar. Tem de saber preparar essa circunstância com simulações, com uma visão das operações, saber quem fala, saber quem faz o quê, saber como se articula isso dentro e fora. Número dois, tem de saber liderar. E liderar significa comunicar nesse momento o que está a acontecer a todos os *stakeholders*. Número três, tem de saber recuperar e comunicar essa recuperação. Fazer o *follow-up* com todos esses *stakeholders* – *media*, clientes, investidores e todos os outros – num período pós, ou seja, semana a seguir, mês a seguir, 6 meses a seguir, 12 meses a seguir, 2 anos a seguir.

Q4: Quais considera ser os desafios atuais enfrentados pelos profissionais de Relações Públicas em situações como esta?

AL: Eu não diria que são desafios. Eu acho que é o ADN de ser um profissional de comunicação pública. A comunicação em si, por definição, é vivida em tempo real e está sempre a mudar. Esses são os desafios de um profissional de comunicação. Tem de saber gerir efetivamente essa cadência, a divulgação dessa informação e tem de ter um compromisso absoluto com a divulgação de uma comunicação factual, transparente e que permita ao público perceber o que se está a passar.

Q5: Já me falou de algumas medidas que os profissionais de Relações Públicas devem implementar. Quer acrescentar mais algumas que sejam realmente importantes em situação de ciberataque?

AL: Vou referir novamente o triângulo que lhe falei: *prepare, lead and recover*. Eu acho que é fundamental para qualquer profissional de comunicação e qualquer empresa preparar a sua organização antes do acontecimento. Isso significa ter uma célula de crise identificada, ter dentro da organização a ideia de quais são os primeiros passos caso aconteça uma situação dessas – com quem se fala, quem é que reúne – para poder libertar o CEO para continuar a liderar o negócio num tempo crítico. Acho que tem de haver um esqueleto, chamemos-lhe assim, de uma célula de crise, que é para poder ser ativada no momento em que isso ocorre. Se for uma situação complicada que precisa de ser avaliada, acho que é preciso considerar chamar uma avaliação externa e independente. Acontece em muitos casos. Portanto, precisa de ser coordenado pelo departamento jurídico, porque na eventualidade de uma crise há sempre limitações e implicações do foro legal. Se for uma situação de ciberataque, deve chamar *forensics*, ou seja, tem de comunicar às autoridades. Também pode chamar *forensics* externos, caso não tenha *in house*, para avaliar o que se passou nos sistemas, para apurar o que aconteceu. E depois tentar perceber o que aconteceu, com esse relatório independente, apresentar ao público interno e externo quais são os *findings*. É sempre bom ter um suporte independente técnico para comprovar aquilo que são os factos recolhidos internamente.

Q6: Anteriormente, também já me falou dos *stakeholders*. Qual considera ser a importância que os *stakeholders* têm numa situação como esta?

AL: Os *stakeholders* são a máxima prioridade, porque são internos e externos. A não ser que a organização prefira esconder – que não é uma opção viável –, a importância dos *stakeholders* começa no minuto em que a falha acontece. Começa pelos seus trabalhadores, pelas suas equipas internamente e vai até aos seus clientes, pacientes, utilizadores, analistas, investidores, *media*. Portanto, é o absoluto dever comunicar aos seus *stakeholders* internos e externos o que está a acontecer.

Q7: Quais considera ser as implicações de um ciberataque para a reputação organizacional?

AL: Tem a ver com a confiança. Ou seja, as implicações são a empresa poder continuar a operar de forma que obtenha a confiança do mercado, dos seus pacientes e dos seus utilizadores ou não. Portanto, a comunicação é fundamental para que todos saibam, de forma transparente e factual, o que está a acontecer. Veja, por exemplo, o caso de uma linha aérea ou uma operadora telefónica, em que a sua base de dados é atacada. O que é que essa empresa faz? No mesmo instante avisar,

por exemplo, os pacientes, utilizadores ou clientes que os seus dados foram comprometidos. Tem de o fazer. Dentro da medida do possível, tem de explicar e chegar às pessoas, para que as pessoas possam efetivamente tomar as suas medidas – mudar as *passwords*, proteger os seus dados –, para que possam ter a confiança da empresa e poder continuar a trabalhar com eles.

Q8: Por último, gostaria de saber quais considera ser os riscos e ameaças do fenómeno do ciberataque para a área das Relações Públicas.

AL: Eu acho que é apenas uma oportunidade, porque acho que é preciso comunicar de forma muito profissional, muito verdadeira, muito factual na eventualidade de um ataque cibernético. Por outro lado, um ciberataque não é "se", mas "quando". Portanto, para as empresas é uma oportunidade saberem acompanhar os seus clientes, aconselhá-los nesses momentos que são difíceis tanto para as organizações, como para quem está envolvido como cliente. Acho que é absolutamente uma necessidade e uma oportunidade para a área das Relações Públicas.

Apêndice 9: Entrevista Carina Sousa Correia

Q1: Fale-me um pouco sobre a sua experiência na área da Comunicação.

Carina Sousa Correia (CC): Comecei a minha carreira no jornalismo, onde passei por vários meios de comunicação social. Mais tarde, entrei na TAP e foi aí – há 16 anos – que comecei a minha viagem pela comunicação corporativa. Foram anos estimulantes em que aprofundei a minha experiência nas mais várias áreas dentro da comunicação organizacional, entre as quais na gestão de crise, relação com os *media, public relations,* comunicação interna, produção de conteúdos e assessoria à equipa de gestão. Saí da TAP a setembro de 2021 para entrar na Vodafone, empresa onde estou, desde então, como *Manager* de Comunicação Externa.

Q2: A Vodafone foi alvo de um ciberataque de grande dimensão em fevereiro de 2022. Gostaria que me falasse um pouco sobre a situação de crise enfrentada pela organização. Qual o modo de atuação da organização perante o incidente?

CC: O nosso maior objetivo – para além de repor a normalidade da operação – era responder objetivamente às questões e inquietações de todos os *stakeholders*. A nossa estratégia passou por conseguirmos ter todos os *stakeholders* elucidados. Acredito que usarmos os mais variados canais (comunicados de imprensa, conferência de imprensa, redes sociais, etc…) para disseminarmos a mesma mensagem foi o que originou um efeito positivo, uma melhor perceção pública da nossa ação. As crises são situações em que tem de haver proximidade com as partes interessadas ao longo de todo o processo, desde a identificação até à resolução.

Q3: Quais as implicações que o ciberataque provocou à organização?

CC: O ciberataque sem precedentes de que a Vodafone foi alvo em 7 de fevereiro de 2022 provocou a destruição intencional de vários elementos centrais das nossas redes, levando a que regressássemos à segunda geração móvel. Serviços de SMS, dados e outros serviços especiais colapsaram e foi necessário, em poucos dias, recuperar o que em "tempos de normalidade" levaria meses. Nas primeiras horas do ataque, foi possível recuperar o serviço de voz móvel, ainda que com constrangimentos e perturbações em algumas ligações e também, embora em modo de contingência, serviços de dados móveis exclusivamente sobre rede 3G. Nas horas e dias seguintes, e faseadamente, recuperámos os restantes serviços: serviços de voz fixa, SMS e serviços de atendimento ao Cliente de voz/digitais. Este foi um trabalho complexo e moroso que nos obrigou, ao longo dessa semana, a estar focados na recuperação total dos nossos serviços. A televisão e o serviço de *Internet* fixa não foram afetados diretamente, mas necessitaram de atividades de estabilização.

Q4: Qual considera ser a importância da comunicação de crise numa situação de ciberataque? Ou seja, o que assegura e o que previne a aposta na comunicação, tanto a nível interno, como a nível externo.

CC: É de extrema importância a equipa de Comunicação Externa ter um contacto próximo, desde o momento zero, com o centro de tomada de decisão, ou seja, com a administração e comité de crise, para definição, priorização e sequenciação de mensagens. Em simultâneo, é importante avaliar todos os fluxos de comunicação – as mensagens disseminadas em todos os canais da Empresa – em permanência, quer interna quer externamente, para garantir:

- internamente, o alinhamento de todos com a informação mais recente e mais útil. A divulgação interna das principais atualizações é fundamental para assegurar a continuidade e tranquilidade dos seus trabalhos, evitando especulações que possam surgir, sobretudo nas redes sociais;
- externamente, as condições de confiança e serenidade junto dos principais *stakeholders* (clientes, fornecedores, parceiros e cidadãos em geral), nomeadamente procurando assegurar informação fiável sobre os tópicos que podem estar relacionados consigo (como, por exemplo, segurança e proteção de dados, restabelecimento da prestação do serviço em condições de qualidade).

Q5: Qual considera ser o papel do profissional de Relações Públicas numa situação de ciberataque?

CC: De forma figurada, é um pouco o eixo de transmissão dentro da organização, que vai tomando conhecimento das principais informações e da evolução da situação, selecionando-as, tratando-as e direcionando-as em função dos destinatários, contribuindo como distribuidor/canal para o que deve ser o desígnio das organizações numa situação como esta: comunicar de forma transparentemente responsável. Qualquer informação passada externamente, transmitida erradamente ou nos canais desadequados, designadamente nas redes sociais, pode pôr em causa as investigações em curso, mas sobretudo a recuperação da continuidade de negócio e a reputação da empresa. Assim, ter *stakeholders* informados e esclarecidos é meio caminho andado para, reduzindo o ruído e a disseminação de informações erradas ou inexatas, permitir à organização concentrar-se na reposição da normalidade.

Q6: Quais os desafios enfrentados pelo profissional de Relações Públicas numa situação de ciberataque?

CC: No geral – e sublinho que neste caso não é o exemplo da Vodafone que está retratado – creio que são de três ordens:

- não ter, do outro lado, um público/opinião pública ciente do que está em causa, o que impede que a mensagem tenha a eficiência necessária e se evitem/superem rumores e desinformação (para combater a desconfiança);
- o desconhecido/imponderável nas primeiras horas após o incidente, que pode gerar/acumular insatisfação e ruído que torne mais difícil uma comunicação eficiente;
- por último, a instabilidade de informação disseminada. Um assessor de imprensa vai sempre procurar responder de forma transparente e mais objetiva possível. No entanto, e com o decorrer do tempo, pode constatar que a informação anteriormente divulgada pode não ter sido totalmente exata. Nesse cenário, é necessário corrigi-la e repor a factualidade, para que a mensagem seja sempre clara.

Q7: Quais as medidas e ações de comunicação que as organizações devem implementar em situação de ciberataque, seja antes, durante e após o incidente?

CC: De um ponto de vista global, o profissional de comunicação "joga" com dois fatores principais no caso de um incidente desta natureza: tempo – sendo exigível que responda e aja rápido – e mensagem – que tem de ser o mais clara e concisa possível. Assim, penso serem necessários, na resposta a um destes incidentes:

- que as relações públicas/comunicação externa possam ter conhecimento permanente das decisões tomadas em comité de crise (que centraliza a gestão de emergência, em articulação com autoridades);
- articulação constante entre os vários intervenientes internos para garantir que se fornece toda a informação necessária e útil a cada momento, enquanto se garante o restabelecimento da continuidade do negócio;
- manutenção de canais permanentes (por exemplo, imprensa, redes sociais, *site* institucional, serviço ao cliente – particularmente de forma personalizada), para que a comunicação possa fluir de forma expedita ao longo de todo o processo, dentro e fora da organização, esclarecendo a cada passo as potenciais dúvidas.

Q8: Qual considera ser a importância dos *stakeholders* em situação de ciberataque?

CC: Fundamental. Internamente, os Colaboradores são indispensáveis, através da sua ação, para recuperar e mitigar os efeitos que o incidente possa provocar – daí que seja necessário que, aqueles que são cruciais para esse restabelecimento, estejam permanentemente na posse da melhor informação possível para desempenhar o seu trabalho; externamente, os Clientes, Fornecedores e Parceiros também têm de estar a par, embora a um ritmo naturalmente menos intenso, da evolução da situação e de como podem ultrapassá-la ou ajudar a ultrapassá-la com a instituição que foi alvo do ataque. Além disso, a própria Opinião Pública no geral merece ser informada, com a mesma transparência, do que sucedeu – desde logo para que, pela partilha de experiências, possa proteger-se e preparar-se para travar ou reagir a um ciberataque.

Q9: A ocorrência de um ciberataque poderá ter implicações na reputação organizacional? Quais são essas implicações?

CC: De uma forma geral, um incidente desta natureza tem consequências negativas na reputação de uma instituição. Pode criar junto dos *stakeholders* uma sensação de apreensão, dúvida ou desconfiança perante a empresa ou organização com a qual tinha uma relação de previsibilidade e na qual se habituou a confiar. No caso da Vodafone, acredito que a relação próxima e de confiança que há mais de 30 anos mantemos com os nossos Clientes foi determinante durante este processo. Contámos com a sua solidariedade e compreensão de que tudo estava a ser feito para repor a normalidade do serviço com a maior brevidade. Foi muito gratificante saber que nesses dias se tinha levantado uma onda de solidariedade, onda essa que nos dava ainda mais força.

Q10: Quais os riscos e ameaças do fenómeno de ciberataque na área das Relações Públicas?

CC: São, em muito, semelhantes aos que acima referi. O risco da desconfiança, o risco da apreensão, o risco da dúvida não esclarecida que, se se prolongarem no tempo, podem deteriorar a imagem pública que clientes e cidadãos têm de determinada organização – o que cria às Relações Públicas desafios de fortalecimento e, por vezes, reconstrução de relações de confiança com as partes interessadas. O maior risco e ameaça está, porém, na impreparação das estruturas para, na eventualidade destes incidentes, responder e resolver da forma mais célere e clara possível. Daí a importância da realização de exercícios e simulações e de uma atualização permanente dos planos de contingência e recuperação.

Apêndice 10: Entrevista Paula Ramos

Q1: Gostaria que a Paula começasse por me falar um pouco sobre a sua experiência na área da Comunicação, em especial da Comunicação de Crise.

Paula Ramos (PR): Eu sou licenciada em Relações Públicas e Publicidade, pelo extinto INP, e desenvolvi toda a minha carreira na área de consultoria em comunicação. Quando falamos em consultoria em comunicação, falamos no trabalho através de agência e onde trabalhamos a comunicação de diversos clientes. Portanto, tudo o que é de seu interesse, tendo muito em vista sempre os seus objetivos de negócio, encarando a comunicação como uma ferramenta para a promoção e para o desenvolvimento do negócio das empresas. Portanto, foi esse o meu percurso ao longo de mais de 20 anos. Em termos de comunicação em contextos de crise, é sempre uma área muito relevante ao nível da reputação das empresas. Isto porque a reputação das empresas é aquilo que nós procuramos sempre trabalhar em comunicação, para que tenham a visibilidade, o reconhecimento, o posicionamento que pretendem para o desenvolvimento do seu negócio, que, como referi, é o princípio máximo. Como é que a questão da crise surge nas empresas? Surge em duas vertentes, muito pela necessidade que existe em determinados contextos de haver uma explicação para o consumidor, para o cliente, para os parceiros, para o próprio público interno de uma situação que está a acontecer e que não é o normal funcionamento da empresa. Portanto, a necessidade que existe de esclarecer os diversos *stakeholders* sobre o contexto em particular. Como é que isto me foi surgindo? A proximidade que nós temos sempre nesta área de consultoria em comunicação com os órgãos de gestão, portanto com as administrações das empresas – muito ao nível de CEO, diretores financeiros, diretores de recursos humanos – é aquilo que leva que, neste tipo de situações, sejamos um parceiro – as equipas de comunicação e a agência, enquanto parte da equipa de comunicação. Portanto, as agências são chamadas a suportar e a orientar a empresa nestes contextos. Ao longo do meu percurso, fiz várias gestões de crise em vários setores,

desde agroalimentar, indústria farmacêutica, numa área mais corporativa… E posso-lhe dizer que foi em várias vertentes. Por exemplo, numa área de *talent*, numa área de recursos humanos, quando estamos a falar, por exemplo, de uma fusão, de uma aquisição, onde temos duas equipas que agora vão começar a funcionar como uma só… Temos também situações de crise com um produto, com um medicamento, por exemplo, em que foi detetada qualquer anomalia, que muitas vezes pode ser só uma anomalia em termos de apresentação e não ter propriamente que ver com o efeito do produto, mas que é necessário tranquilizar os consumidores e os prescritores de que está tudo ok. Portanto, esse esclarecimento que é feito com os diversos *stakeholders*, uma vez mais. E nesse tipo de situações, por exemplo, um *stakeholder* muito considerado são os *media*, enquanto veiculadores de mensagens e informação. Portanto, foram várias as situações que me foram surgindo ao longo destes 20 e tal anos de experiência. O meu percurso resume-se a duas agências: a LLYC, onde estou atualmente, e a Lift, onde estive durante 20 anos. Foi na Lift que eu desenvolvi grande parte dos projetos de crise em que estive envolvida. E na LLYC foi um percurso muito a par do desenvolvimento diria, também, da área de comunicação. Eu entrei na Lift em 1997, penso eu, onde estive até 2018. Durante este tempo, eu fiz todo o percurso possível dentro de uma agência. Portanto, entrei como estagiária, assumi primeiro uma conta, depois fui integrando uma equipa, liderando a minha equipa enquanto diretora de comunicação, depois, mais tarde, liderando várias equipas e, neste caso, assumindo já a direção executiva… Portanto, quando eu saí em 2018, tinha já a direção-geral a meu cargo. Eu saí porque quis, de facto, fazer aqui um *break*, que às vezes também é importante. Mas mantive sempre uma ligação muito próxima numa lógica de *freelancer*, mas com alguns projetos que fui fazendo com algumas agências. E comecei, também, uma área muito próxima da área de crise que eu costumo dizer que é uma área de pessoas, porque pessoas e crises estão sempre muito interligadas… E faço, desde então, consultoria de carreira, portanto gestão e orientação de carreiras de profissionais. E depois surgiu o convite da LLYC, há uns meses atrás, para assumir a direção da área corporativa e financeira, com um enfoque na área da saúde.

Q2: Qual considera ser a importância da comunicação de crise numa situação de ciberataque?

PR: Há duas formas de nós vermos a crise. Numa crise surgem sempre oportunidades e eu acho que, em contexto de ciberataque, devemos sempre perceber o que podemos aprender com essa situação. Mas uma crise nunca é uma situação boa, porque o fluxo normal de trabalho, por alguma razão, foi descontinuado. E há sempre duas formas de vermos isto. Por um lado, a prevenção, que é o que, para mim, pode de facto fazer uma boa gestão de crise, ou seja, uma crise pode ser tão bem gerida quanto melhor preparados para ela estivermos. Portanto, há um momento de prevenção de crise, em que temos de equacionar os diversos cenários que podem surgir ou o que é que pode

ser uma crise. Por exemplo, considerando um ciberataque – tivemos vários recentemente e vamos continuar a ter –, o que é que pode acontecer? Pode ser uma falha de energia, pode ser um *hacker* que ataca os servidores, pode ser uma má utilização, porque também há muita falha humana em tudo o que são crises, pode ser uma utilização indevida também do próprio sistema informático… Portanto, há um determinado número de contextos que podem existir e que devem ser identificados à partida. Havendo essa prévia identificação, deve-se perceber, numa situação destas, o que é que eu tenho de fazer, quem é que eu tenho de ativar, o que é que eu devo dizer, o que é que eu posso dizer… Nunca mentir é uma regra, mas dizer tudo, por vezes, também não é a solução. Portanto, é preparar devidamente o tipo de mensagens, identificar e mapear perfeitamente não só os *stakeholders* a quem nós queremos fazer chegar a nossa informação, mas também aqueles que nós, a determinado momento, podemos querer "utilizar" para fazer a nossa comunicação, sejam parceiros, associações ou outro tipo de *stakeholders* que nos possam ajudar nesta gestão. Esta identificação deve ser revista regularmente – na minha perspetiva, no mínimo uma vez por ano –, isto porque entretanto muda um número de telefone, muda uma pessoa, o que quer que seja… Deve-se fazer, portanto, alguns simulacros, ou seja, percebermos mesmo, numa situação destas, como é que isto funcionaria. Não basta olhar para o documento e perceber que o número de telefone está lá. A pessoa associada ao contacto está preparada para ser o *speaker*? Tem as condições necessárias em casa, sobretudo agora com o remoto? Tem rede? Todas estas coisas que nos parecem pequenos detalhes, no momento podem falhar. Por exemplo, um dos aspetos fundamentais numa situação de crise relaciona-se com o facto de hoje estarmos todos no digital, mas se houver uma falha de energia não consigo aceder a um documento digital. Portanto, um manual de crise é importante que exista sempre impresso, que exista sempre em papel um ou dois exemplares, porque têm de ser considerados. Isto num momento de prevenção… Numa situação de crise, o objetivo será ativar tudo isto, ou seja, a resiliência das pessoas, as pessoas devidamente identificadas, manter a calma para reagir a este tipo de situações, que são situações de pressão, de tensão e onde nós estamos sempre em prejuízo, não é? Porque houve algo errado que aconteceu, portanto nós vamos estar a correr atrás do prejuízo, ou seja, temos um problema para resolver. Quando fazemos um bom trabalho de prevenção, a vantagem que temos é que estamos sem essa pressão adicional, porque não está a acontecer nada de grave, portanto podemos ter ali o *test and fail* e perceber se isto ou aquilo funcionaria. No contexto particular de cibersegurança, eu diria que o maior risco ou risco adicional que podemos ter aqui, muitas vezes, é a visibilidade que isto tem e os impactos. Estamos a falar de entidades que têm um conjunto de empresas, muitas vezes, que ficam com os serviços condicionados e a visibilidade que tudo isto tem. Não considero que uma situação de cibersegurança seja muito pior que outras situações. Se nós pensarmos numa situação alimentar, se nós pensarmos numa situação de uma medicação que não está a ter os efeitos

previstos ou, inclusive, está a ter efeitos nocivos… Tudo isto são situações de crise, naturalmente. Portanto, é sempre um problema. Para mim a questão do ciberataque é uma situação que tem muita visibilidade e, como tal, afeta muito a reputação da empresa e esse é o ponto que nós deveremos sempre ter de proteger ao máximo. Tem uma visibilidade que, se calhar, não tem se houver, imagine, uma situação de intoxicação alimentar num refeitório de uma escola. Tudo bem que são crianças, mas estamos ali confinados àquelas crianças daquele refeitório, portanto a abrangência não é tão grande. Num ciberataque, normalmente, estamos a falar de uma dimensão completamente distinta.

Q3: A Paula já me falou várias vezes da reputação organizacional. Quais considera ser as implicações que um ciberataque, sobretudo de grande magnitude, pode ter na reputação das organizações?

PR: As implicações podem ser várias e de diferentes amplitudes. Por exemplo, quando nós temos uma situação de ciberataque em que a empresa diz "não sabemos o que se está a passar", "os nossos clientes estão em segurança", "não houve partilha de dados", "não houve acesso a informação confidencial", ou seja, não há certezas do que aconteceu, isso é sempre um problema. Para mim, o grande truque – se é que lhe podemos chamar um truque, que eu acho que é um truque de vida – é sermos verdadeiros. É preferível dizer "ainda não temos noção da amplitude", "estamos a averiguar", "estamos a encetar todos os esforços para perceber o que se está a passar"… É preferível dizermos isto do que estarmos a dizer "não, nada aconteceu". Quando muito, podemos dizer "até ao momento, não temos informação de que exista partilha de dados dos nossos clientes", "até ao momento, o que nos é permitido averiguar é que estamos neste e neste ponto". Portanto, este para mim será sempre o ponto, que é não assumirmos coisas das quais não temos certeza, porque se nós dissermos isto e se vier a confirmar, a confiança fica automaticamente fragilizada. Ou seja, a mim dizem-me "não houve corrupção de dados, portanto os dados dos clientes estão protegidos" e passado meia hora, uma hora ou uma semana vem-se a comprovar que os dados, de facto, foram acedidos, é natural que haja uma quebra de confiança grande. Para mim, a reputação será sempre tão mais assegurada e tão mais mantida… Eu não diria que as empresas ficam com uma melhor reputação após uma boa gestão de crise, mas pelo menos não ficarão pior. Verdade, dar a cara, assumir-se um compromisso em que, de hora a hora, se dá um *feedback* ou explica o ponto de situação… E nem que seja um ponto de situação para dizer "até agora, não temos mais informações relativamente ao *status* anterior", mas demos a cara, não nos escondemos. Esse, para mim, será sempre o ponto que pode marcar e que marcará a diferença de uma boa ou de uma má gestão e manutenção de reputação.

Q4: Qual considera ser a importância dos *stakeholders* numa situação de ciberataque?

PR: É fundamental. Os *stakeholders* são todas as partes interessadas e, portanto, estamos a falar de clientes, estamos a falar de parceiros, estamos a falar de fornecedores, estamos a falar do *stakeholder* interno, atenção, é um *stakeholder* muito relevante. Um *stakeholder* interno é um *stakeholder* que funciona muito, também, como embaixador. Quando nós ouvimos falar de uma empresa ou queremos ir trabalhar para uma empresa, a primeira coisa que nós tentamos saber é se conhecemos alguém que trabalhe lá dentro ou que já tenha trabalhado com essa empresa. Ou seja, nós procuramos também pelas vias informais ter acesso a alguma informação, além do que é publicado e acessível a toda a gente. A partir do momento em que eu tenho um *stakeholder* interno que tem informação – uma vez mais, não tem de ter toda a informação, mas tem de ter informação que é divulgada e pode funcionar como um embaixador que desconstrua ou passe uma visão de transparência da empresa. Portanto, numa situação como esta, sentir que o *stakeholder* interno está tranquilo e que, com essa sua tranquilidade, consegue passar também essa segurança para o exterior é fundamental. Portanto, dizer-lhe que o mapeamento de *stakeholders* é dos trabalhos mais importantes a ser feito numa situação de prevenção de crise e numa situação de gestão de crise. Não esquecer a concorrência, que também pode, por vezes, aproveitar – não é muito habitual, pelo menos em Portugal – uma situação de maior fragilidade.

Q5: No âmbito das organizações, qual considera ser o papel do profissional de Relações Públicas numa situação de ciberataque?

PR: Eu diria que o principal papel de um profissional de Relações Públicas… É assim, normalmente as empresas têm gabinetes de crise e, nestes gabinetes, o profissional de Relações Públicas – ou profissional de comunicação, gosto mais da expressão – é um dos elementos. Mas esse gabinete, normalmente, é liderado pelo presidente da empresa ou pelo CEO ou por alguém da área. Por exemplo, na área agroalimentar é muito normal este gabinete de crise ser liderado por alguém da medalha de segurança e qualidade alimentar, independentemente das crises, às vezes, não estarem relacionadas com a área, até pode ser um ciberataque. Mas, muitas vezes, esta pessoa é o diretor do gabinete de crise. Depois, o que faz, de acordo com a área que é o alvo da crise, é ir acionando as pessoas de todas as áreas. Normalmente já existe uma pessoa definida. Numa situação de ciberataque, como em qualquer outra situação de crise, o profissional de comunicação é alguém que lá está, que faz parte deste gabinete, e que tem aqui o papel fundamental de manter a calma e de orientar todo o processo de comunicação. Porque, numa situação de crise, temos sempre duas vertentes. Temos a vertente da comunicação no contexto de crise. E temos a própria vertente de crise, numa ótica mais técnica, de resolução. Portanto, o profissional de Relações Públicas não será, numa situação de ciberataque, quem está a tratar da parte tecnológica, da parte

de segurança. Mas deverá ser quem permite que a pessoa responsável por fazer isso o faça com a maior das serenidades, tentando evitar contactos com jornalistas, concentrando em si todos esses contactos, a definição das mensagens-chave, ter um bom documento de Q&A, portanto perguntas e respostas expectáveis e ir trabalhando sempre esse documento. É um documento que deve estar em atualização permanente, porque às vezes a pergunta mais tonta – que nós achamos que ninguém vai perguntar – surge. E as perguntas tontas, por vezes, têm exatamente essa habilidade que é, como não são previstas, de nos desarmarem. Portanto, devemos equacionar todas as questões, desde as mais tontas às mais inteligentes, para estarmos, de facto, preparados para tudo. Perceber também que, muitas vezes, em termos de *media*, quem trabalha numa situação de crise não tem de ser propriamente o jornalista que acompanha a empresa ou que está mais próximo da empresa ou do setor. Porque uma situação de crise é algo que surge e imagine que esse jornalista está de férias ou não está a trabalhar naquele turno… Portanto, temos previsto que estas questões todas podem, de facto, surgir, porque a pessoa que pega no assunto, se calhar, é um jornalista de uma outra área que não tem o contexto. Portanto, é muito importante ter esta documentação toda preparada e o profissional de comunicação deve ter, de facto, isto. Deve ter devidamente validado logo todos os procedimentos de segurança que existe, ou seja, dizer "a empresa x tem este e este processo de segurança e estes são os protocolos que nós seguimos, as medidas que nós efetuamos sempre, todo este trabalho tem sido feito, houve aqui uma intrusão, houve aqui uma falha, mas até às 10h desta manhã foi feito o último *backup*, portanto toda a informação está salvaguardada, o ataque foi às 11h30 e o próximo *backup* só será feito às 10h da manhã do dia seguinte". Ter esta informação toda em seu poder é muito importante. Uma vez mais, a forma como nós a colocamos e a forma como nós a divulgamos terá de ser visto situação a situação. Ou seja, o facto de eu há pouco estar a referir que tem de haver transparência e clareza na mensagem não quer com isso dizer que devemos dizer tudo a toda a gente e a toda a hora, de todo. Temos é nós, para liderarmos a crise, ter a informação do nosso lado. É a diferença entre liderarmos e sermos liderados. Porque, lá está, se eu digo que não houve invasão dos dados e, de repente, até houve… isto é que não pode acontecer. Portanto, eu tenho de ser o detentor da informação certa, fidedigna e verdadeira.

Q6: Numa situação de ciberataque, quais considera ser os principais desafios enfrentados pelos profissionais de Relações Públicas?

PR: Os desafios enfrentados numa situação de ciberataque eu diria que, muitas vezes, poderão ser a quantidade de coisas e de pequenos detalhes a que uma empresa poderá ser exposta. Isto porque há muita informação numa empresa, está tudo informatizado… portanto, eu diria que esse poderá ser um dos grandes desafios. Talvez um dos maiores desafios é percebermos qual foi o nível de intrusão que houve, o que é que de facto ficou em risco… pode também ter havido alguma

passagem de dados incorretos de uma área para outra área. Imagine que existe uma área de clientes, onde temos uma informação dos preços de venda, existe uma alteração desses dados e, de repente, o produto começa a ser vendido a um preço completamente diferente ou começa a ser dado como disponível e não está… daqui podem advir as ditas crises. Portanto, eu diria que o grande desafio aí é tão rapidamente quanto possível perceber o que é que está, de facto, em causa, o que é que está, de facto, em risco e até que ponto uma área não irá afetar outra. Isto pela interligação e pela interconexão que existe hoje em dia em termos de informação.

Q7: A Paula já me tem vindo a falar sobre algumas medidas e ações de comunicação que as organizações devem implementar na resposta a um ciberataque. Quer acrescentar mais alguma?

PR: Numa situação de crise, eu diria que o principal ponto a ter em conta será mesmo ter a informação toda preparada e fazer uma reunião do gabinete de crise, para perceber qual é a situação em que estamos. Antes de mais, mapear. Esta é a situação em que estamos. Esta situação vai impactar o quê? Quem são os *stakeholders* que vão ser impactados com isto? *Next step*: qual é o ponto que podemos vir a ter daqui a uma ou duas horas? Poderá ter impacto em quê? O que é que eu consigo, desde já, em termos de sistemas, eventualmente prevenir bloquear para que a crise não venha a escalar? Acho que é importante termos uma boa preparação das pessoas. A definição dos *speakers*, das pessoas que vão dar a cara e a preparação destas pessoas… E dar a cara não significa ter de ir para a televisão fazer grandes declarações, pode ser um *statement* que é enviado e que é divulgado. Mas as pessoas que vão ser aqui utilizadas e a quem vamos recorrer para fazer esta comunicação devem estar preparadas – é fundamental. Como já referi, a prevenção é a melhor arma, de facto. E depois acho que, após uma situação de crise, há sempre uma aprendizagem grande que pode ser feita, que é percebermos o que aconteceu, porquê que aconteceu, o que é que nós poderíamos ter feito de diferente – e haverá sempre coisas que podem ser feitas de forma diferente – e o que é que temos agora de alterar no nosso sistema, na nossa formação, nos nossos procedimentos para que não volte a acontecer. Os simulacros são também algo que ajuda bastante, porque é quando nós nos vemos o mais próximo possível de uma situação destas. E aqui temos vários pontos que nos podem parecer coisas menores, mas não são, que é a rapidez na resposta, o responsável do gabinete de crise tem de ter o telefone sempre ligado, porque se acontece às onze da noite e, se não tem resposta, pode vir para fora sem resposta da nossa parte – e não há nada pior do que tentar contactar a empresa e não ser possível obter qualquer declaração… quando nós temos isto dos *media* é complicado ou quando temos isto, de facto, a criar impacto na vida das pessoas. Portanto, eu diria que cuidados a ter é preparar, acho que o melhor que podemos fazer é preparar as crises, em termos de mensagens, *stakeholders*, simulacros, etc. Durante uma crise, é muito

manter a calma, a resiliência, termos a capacidade de pensar de cabeça fria, termos a capacidade de envolver todas as pessoas que nos possam aportar algum conhecimento e alguma informação para uma boa resolução, mas mantendo sempre uma liderança firme e segura. E num pós-crise, é claramente avaliarmos a crise, o que aconteceu, o que poderíamos ter feito de forma diferente, para que da próxima vez que vier a acontecer – porque vai voltar a acontecer, é perfeitamente normal e não é expectável que deixem de acontecer este tipo de crises, ainda mais numa área de cibersegurança, porque o que está em grande desenvolvimento é normal que aconteça – como é que eu consigo mitigar os riscos da melhor forma, para que tenha o menor impacto e a menor visibilidade. Porque quer uma situação, quer outra, vão impactar muito a reputação da empresa. Mesmo que não seja algo que tenha uma visibilidade pública, a partir do momento em que alguém que utiliza um serviço, que é cliente sente isso… o cliente é claramente um *stakeholder* que tem de ser levado em conta e percebermos como é que ficou, fazermos um acompanhamento, já terminámos, os sistemas já estão todos operacionais… Diga-me, por favor, os impactos que isso teve no seu negócio? Como é que foi? Sentiu dificuldades? Como é que foi a vossa capacidade de resposta? Termos a capacidade de recolher *feedback* neste tipo de situações é extremamente relevante.

Q8: Por último, quais considera ser os riscos e ameaças do fenómeno de ciberataque na área das Relações Públicas? Ou seja, se vai impactar de alguma forma aquilo que era, até então, a área das Relações Públicas.

PR: Eu acho que impactará a partir do momento em que as empresas de Relações Públicas são empresas. Nesse impacto, poderá ter isso. O que é que os ciberataques têm para que possa impactar a atividade? Eu diria que é um bocadinho o contexto da rapidez com que as coisas acontecem. Mas eu diria que isso tem que ver com ciberataques ou com qualquer outra atividade. Há 20 anos atrás, quando eu comecei a trabalhar nesta área de crise, nós não tínhamos redes sociais… os próprios *timings* tiveram de ser adaptados, nós não tínhamos meios *online*… quer dizer, há 20 anos já tínhamos um ou outro, mas há 25 não tínhamos. Nós não tendo meios *online*, fazia-se a gestão para o dia seguinte. Agora não, tem de se fazer para o minuto seguinte. E pensar que toda a gente tem uma presença digital e que toda a gente é um *stakeholder*. A partir do momento em que eu tenho um *Facebook*, tenho um *Instagram*, tenho um *LinkedIn* e que dou acesso a que qualquer pessoa me siga e possa ir lá fazer um comentário, os próprios *timings* de gestão das crises têm de ser adaptados, têm de ser geridos.

Q9: Penso que conseguimos abordar todos os tópicos que estavam previstos inicialmente. Não sei se a Paula quer acrescentar mais alguma ideia que considere relevante e que não tenhamos abordado.

PR: A cibersegurança é claramente uma área muito importante, porque qualquer empresa, hoje em dia, está sujeita a sofrer um ciberataque, porque a tecnologia é transversal a todas as empresas. Portanto, eu diria que é das áreas que as empresas mais têm de ter em linha de conta, perceber como é que têm protegidas as suas redes, as suas informações. E então cada vez mais, se já assim era no passado, tivemos uma pandemia que ainda nos pôs mais remotos e ainda nos pôs mais digitais. Portanto, o que eu diria é que, de facto, é uma das áreas *core*, hoje em dia, a considerar e eu diria que todos os bons manuais de gestão de crise deverão contemplar logo como prioritário um ciberataque.

Apêndice 11: Entrevista António Borges

Q1: Gostaria que o António começasse por me falar um pouco sobre a sua experiência na área da Comunicação.

AB: Eu sou licenciado desde 2004, salvo erro – já são alguns aninhos em Comunicação e Relações Públicas – pela Escola Superior de Educação do Instituto Politécnico da Guarda. Já desde os meus 15 anos que estou ligado, de certa maneira, àquilo que é a atividade de emergência médica e pré-hospitalar… Fui bombeiro voluntário durante muitos anos. Depois de já estar licenciado, acabei por ingressar no Instituto Nacional de Emergência Médica enquanto técnico de emergência pré-hospitalar, tendo exercido essas funções durante cerca de 10 anos até ano de 2017, altura em que, por vicissitudes diversas da vida, acabei por transitar para o Gabinete de Comunicação e Marketing do Instituto, aliando, assim, aquilo que era a minha formação académica e também aquilo que era a minha experiência profissional enquanto conhecedor e técnico de emergência pré-hospitalar. Portanto, juntei o percurso académico àquilo que era a minha experiência profissional e aqui estou, atualmente, a exercer funções enquanto Técnico Superior de Comunicação e Marketing no Gabinete de Comunicação e Marketing do INEM.

Q2: Relativamente ao ciberataque que o INEM sofreu em dezembro de 2022, gostaria que o António me falasse um pouco sobre a situação de crise enfrentada pela organização. Qual o modo de atuação do INEM perante o incidente?

AB: Aquilo que aconteceu, sem entrar em grandes pormenores – até porque pormenores a nível técnico do próprio ataque eu também não os conheço ao seu detalhe –, é que houve um comprometimento através da divulgação de credenciais de acesso àquilo que era uma plataforma

que o INEM utilizava. Com o ciberataque, essas credenciais foram expostas. Assim que o INEM teve conhecimento, através do gabinete de sistemas e tecnologias de informação, tomou todas as medidas que são necessárias, nomeadamente a revogação dos acessos, a comunicação ao Centro Nacional de Cibersegurança e verificar até que ponto esse ataque tinha afetado aquilo que é a atividade do INEM. Após feita essa análise, chegou-se à conclusão de que aquilo que é o *core business* do Instituto, ou seja, a prestação de cuidados de emergência médica pré-hospitalar não tinha sido afetada, portanto os danos não foram significativos para aquilo que era a atividade principal do Instituto e que, de facto, poderia provocar alguns constrangimentos. Depois de termos conhecimento da extensão dos danos, houve a necessidade de comunicar isso à população e assegurar que a atividade do INEM – aquela que tem mais impacto nas pessoas, que é a prestação de cuidados de emergência pré-hospitalar, através do sistema integrado de emergência médica – não tinha sido comprometida. Isso foi feito através da divulgação de um comunicado de imprensa, através dos órgãos de comunicação social e também através da nossa rede social *Twitter*. E foi isto basicamente que foi efetuado.

Q3: Quais as implicações da ocorrência do ciberataque para a organização?

AB: Houve certamente medidas que foram tomadas pelo gabinete de sistemas e tecnologias de informação que foi, conforme já lhe disse, verificar quais foram os danos que, no fundo, foram provocados e não foi afetado aquilo que era atividade principal. Houve, salvo erro, uma plataforma de formação *online* que foi afetada e esteve inativa durante algum tempo. Portanto, houve esse trabalho por parte desse gabinete do Instituto em verificar e tornar novamente os acessos seguros e tudo aquilo que é o mundo digital que rodeia toda a nossa atividade… verificar até que ponto estava seguro e isso foi feito no imediato, nos dias seguintes.

Q4: Numa ótica mais geral, qual considera ser a importância da comunicação de crise numa situação de ciberataque? Ou seja, o que assegura e o que previne à organização a aposta na comunicação, tanto a nível interno, como a nível externo.

AB: A comunicação de crise no INEM é algo que está bastante presente e é fundamental, porque o INEM é um instituto que tem uma atividade de muita importância para a vida das pessoas. Ou seja, nós, em conjunto com os nossos parceiros do sistema integrado de emergência médica da prestação de cuidados de emergência pré-hospitalar, somos responsáveis por ajudar as pessoas em momentos, por vezes, de maior necessidade e de maior aflição. E há, de facto, aqui um conjunto de situações que pode impactar essa atividade. Portanto, é comunicação de crise quando elas acontecem, nas mais diversas formas… é importante nós conseguirmos assegurar às pessoas se essa atividade está ou não está assegurada, está ou não está comprometida, está ou não está posta

em causa. É fundamental conseguirmos falar com as pessoas, transmitir as informações e assegurar às pessoas que, se precisarem de uma ambulância em caso de acidente ou doença súbita, têm ou não têm acesso a ela. Portanto, a comunicação de crise é algo que nós temos muito presente no nosso dia-a-dia no Instituto, porque as crises que podem afetar a instituição e a confiança que as pessoas têm na instituição são muitas e, portanto, é importante que isso seja assegurado. A nível interno também é importante, porque o Instituto, como o próprio nome indica, é nacional, portanto trabalha desde Vila Real de Santo António até Valença do Minho, temos meios espalhados por todo o território continental. E chegar aos nossos públicos internos, aos nossos trabalhadores que estão espalhados por Portugal fora nem sempre é fácil. Por vezes, as pessoas podem ter conhecimento de alguma notícia menos boa ou de alguma potencial crise não pelos meios oficiais, digamos assim, e é importante nós também termos canais de comunicação internos bem estabelecidos, para que, em caso de crise ou de uma potencial crise, os nossos trabalhadores, que são a nossa cara junto das pessoas, estejam informados e tenham presente aquilo que se está a passar, para, também eles, poderem assegurar ou não aquilo que se passa e informar as pessoas convenientemente.

Q5: Qual considera ser a importância de todos estes *stakeholders* numa situação de ciberataque?

AB: Os *stakeholders* do INEM, qual é a importância deles? É fundamental, porque o INEM não trabalha sozinho. O INEM trabalha com um conjunto vastíssimo de entidades, sejam elas governamentais, como é o caso do Ministério da Saúde ou hospitais, e até entidades privadas, como, por exemplos, os corpos de bombeiros voluntários onde nós temos postos de emergência médica. Portanto, é fundamental também comunicarmos com essas pessoas e essa comunicação ser feita, para que este trabalho em rede que o INEM tem esteja sempre garantido.

Q6: Qual considera ser o papel do profissional de Relações Públicas numa situação de ciberataque?

AB: O trabalho do profissional de Relações Públicas nestas situações de crise é fundamental, porque, no fundo, nós somos aquele elemento de charneira que está ali para comunicar de forma eficaz com os diversos públicos aquilo que se está a passar. Obviamente que não foi o gabinete de sistemas e tecnologias de informação, no caso do ciberataque, que comunicou ao público externo diretamente aquilo que se estava a passar. Fomos nós, através de informação que recebemos desse gabinete, que depois tivemos de transformar a mensagem que, por vezes, é técnica, para que seja percetível para um público geral e mais abrangente. Portanto, é esse o nosso trabalho, fazer esta

articulação com os diversos públicos, transmitir as mensagens e, assim, fazer uma eficaz comunicação de crise.

Q7: Neste papel que o profissional de Relações Públicas desempenha em situação de ciberataque, quais considera ser os principais desafios enfrentados?

AB: O principal desafio, enquanto profissional de Relações Públicas e o tal elemento de charneira, ou seja, esse ele de ligação entre a fonte de informação e o público, é garantir até que ponto a informação que nós recebemos é precisa e correta, para depois garantir que aquilo que vamos comunicar é uma informação completa e que não tem falhas. Porque, depois, o mais chato é nós transmitirmos uma informação que não está completa e depois sermos confrontados, por exemplo, pela comunicação social com algo que nós desconhecemos. Isso depois põe em causa aquilo que é a confiança que as pessoas depositam em nós. Portanto, esse é um dos desafios, que é nós termos a certeza de que estamos munidos de toda a informação, para depois podermos fazer, então, uma comunicação que consideramos completa e eficaz. Outro dos desafios é precisamente perceber aquilo que se está a passar, é ter o mínimo de conhecimento técnico, é saber como funciona a área em que estamos a trabalhar, para que, caso haja alguma questão, nós também sabermos responder.

Q8: Numa situação de ciberataque, quais considera ser as principais medidas e ações de comunicação que as organizações devem implementar, seja antes, durante e após o incidente?

AB: Em termos gerais, aquilo que temos de fazer para prevenir um ciberataque é informar as pessoas daquilo que são os bons hábitos que deve adotar quando navegam no espaço digital do Instituto, como, por exemplo, o uso correto de *passwords*. Portanto, é um trabalho prévio de prevenção que nós fazemos juntamente com o gabinete de sistemas e tecnologias de informação, para informar os colaboradores acerca daquilo que são os comportamentos seguros que ajudam a prevenir a ocorrência desses ciberataques. Mas lá está, é informação que vamos buscar e que o *chief security officer* nos transmite e que nós depois divulgamos nos nossos meios de comunicação internos, como a nossa *newsletter* diária. Muito importante, também, é ter o planeamento minimamente feito. Se acontecer um ciberataque, o que é que eu devo fazer? Primeiro, é perceber até que ponto esse ciberataque pode ou não impactar aquilo que é a atividade da organização. E depois, mediante esse impacto e a gravidade dos danos causados pelo ciberataque, obviamente que se tem de estabelecer um plano de ação e informar os *stakeholders*… E depois, lá está, em situações mais graves, no caso do INEM, fazer uma informação geral ao público, tranquilizar as pessoas, como foi o caso da situação que se passou em dezembro de 2022, que foi, de facto, informar as pessoas que a atividade do INEM não tinha sido posta em causa. No fundo, é perceber a extensão

dos danos e informar, mediante essa extensão, as pessoas que são afetadas ou não, porque se for uma crise de pouca dimensão ou pouca expressão, se calhar também não faz sentido estar a levantar alertas que podem vir a ser desnecessários. Obviamente que a comunicação deve estar sempre presente durante todas as fases de uma crise – antes, durante e depois –, por isso depois da crise acontecer é importante fazer o acompanhamento da situação, verificar se a situação está ultrapassada, se há problemas que estejam a ser vividos e que mereçam, ou não, algum tipo de informação ou de complemento de comunicação que ajude a ultrapassar a crise e a prevenir que situações idênticas ocorram novamente. E isto acaba por ser um ciclo, não é? Retiram-se lições aprendidas e tenta-se comunicar de forma que não se voltem a suceder no futuro.

Q9: Considera que um ciberataque pode ter implicações na reputação organizacional?

AB: Claro que sim, claro que pode. Vamos ver, há exemplos que são conhecidos de pessoas que têm as *passwords* de acesso coladas com post-its no monitor do computador… Portanto, quando isso é do conhecimento público não transmite propriamente uma boa imagem da organização no que diz respeito à cibersegurança. Demonstra até algum desleixo daquilo que deviam ser as funções dos funcionários da organização. Portanto, obviamente que tem impacto para a reputação da organização um ciberataque. Uma empresa que não tenha ciberataques, no mundo atual, é talvez uma empresa que tem uma reputação um bocadinho mais alta no que diz respeito a isso… Porque tem medidas implementadas que permite ser cibersegura.

Q10: Por último, quais considera ser os riscos e ameaças do fenómeno de ciberataque na área das Relações Públicas?

AB: Um ciberataque pode provocar uma crise mediática, mas não deixa de ser uma crise, a origem é que é diferente. Portanto, acredito que um ciberataque é só mais um fator que um profissional de Relações Públicas tem de estar desperto para que possa acontecer e poder ter de lidar com as suas implicações. Portanto, obriga a que haja um conhecimento adicional, de uma área que, até há pouco tempo atrás, não era uma realidade tão presente. Mas, no fundo, a crise que pode surgir e a forma de a ultrapassar não deixa de ser idêntica a todas as outras. É "só" mais uma crise que estamos de estar preparados para lidar. Obviamente que se queremos ser bons comunicadores e lidar bem com essa crise, obriga-nos a fazer um pouco o trabalho de casa, conhecer o léxico, como é que funcionam os sistemas informáticos, etc. No fundo, acho que é isso.

Apêndice 12: Entrevista Rui Cabrita

Q1: Gostaria que o Rui começasse por me falar um pouco sobre a sua experiência na área da Comunicação.

RC: O meu percurso profissional de quase 30 anos de comunicação tem várias vertentes. Eu sou de economia, licenciei-me e tenho mestrado em economia. Fui parar à comunicação por um acaso. Portanto, fui parar ao jornalismo… durante 12/13 anos, fui empreendedor e jornalista na área de economia, quer no Jornal de Negócios, quer depois no Diário Económico. E depois, em 2006, fui convidado para vir, então, para a EDP para o departamento de comunicação. Na altura, apenas como assessor de comunicação e depois, enfim, fui evoluindo na carreira, fui ganhando competências, fiquei com a comunicação interna também… Portanto, hoje em dia, sou Diretor Global de Comunicação do Grupo EDP, responsável por todas as geografias do Grupo EDP, obviamente com equipas locais e tenho a responsabilidade de toda a cadeia de valor da comunicação: comunicação interna, comunicação externa, comunicação digital, gestão de redes sociais, gestão de *sites* corporativos, relação com os *media*, comunicação de crise… Enfim, tudo o que é comunicação está debaixo da minha responsabilidade. Nós aqui na EDP – e não é assim em todas as empresas – temos a gestão da marca noutra direção que é a Direção de Marca. Obviamente que há aqui zonas que se tocam, obviamente que há uma grande coordenação entre as duas direções, mas digamos que há uma Direção de Marca e há uma Direção de Comunicação. Eu sou o Diretor Global de Comunicação e estou na EDP, portanto, desde 2006.

Q2: A EDP foi alvo de um ciberataque em abril de 2020. Tendo por base esse incidente, gostaria que o Rui me falasse um pouco sobre a situação de crise enfrentada pela EDP. Qual foi o modo de atuação da organização perante o ciberataque?

RC: Na gestão de crise de um ciberataque ou na gestão de crise de outra situação, a cartilha é quase a mesma. É algo inusitado, naturalmente, que não se está à espera, por isso é que é crise. E eu já apanhei várias situações de crise, desde furacões que destruíram e que deixaram metade do país às escuras, desde pessoas que sofrem acidentes e que morrem numa barragem… enfim, várias situações de crise e onde se inclui também, obviamente, este ciberataque que ocorreu nessa altura. Portanto, obviamente que nós temos uma planificação, há um manual de gestão de crise – não especificamente para ciberataques – que define um conjunto de procedimentos e um conjunto de atuações que nós, obviamente, em situação de crise tentamos seguir. Mas, por se tratar de uma situação de crise e porque, por vezes, a resposta tem de ser ágil, na verdade, por vezes, acabamos por não ir lá ler o livro. O que é que é importante? Há aqui várias frentes e a comunicação é apenas uma delas. A comunicação em situações de crise não vive por si só. Já em crise, há um conjunto

de articulações que tem de ser feito, nomeadamente articulação com os principais *stakeholders* da crise. No caso do ciberataque, é importante falar com as autoridades, falar com os polícias, falar com o Centro Nacional de Cibersegurança… Eles, no fundo, é que têm o *know-how* desta área. Porque isto envolve muitas situações… Eu recordo-me que, no nosso caso, eles pediam dinheiro para não divulgarem informação. Obviamente que há aqui um período em que é fundamental, nos ciberataques, nós percebermos qual é que é exatamente a extensão do ataque – foi esta a minha experiência e foi o que eu mais recolhi dessa altura. Nós, a determinado momento, percebemos que os dados que eles tinham tido acesso eram dados desatualizados, antigos e que não punham em causa a divulgação de dados confidenciais – ou, pelo menos, os dados confidenciais que eles tinham eram já desatualizados. Portanto, o risco era mínimo, era um risco controlado, mas nós não tínhamos a certeza se eles tinham mais dados ou não. Aquilo era o que nós conseguimos ter acesso, mas não sabíamos se eles depois tinham mais dados que, de alguma forma, logo a seguir nos pudessem expor mais a situação. Portanto, eu diria que numa situação de crise – em qualquer crise, mas também em ciberataque –, do ponto de vista de comunicação, a primeira coisa é ter alguma frieza. Não ir muito ao arrasto daquilo que é o drama. Manter aqui alguma frieza e tentar perceber exatamente o que é que está em causa, qual é a extensão. E isso não depende da comunicação, depende das áreas técnicas, depende dos nossos colegas das áreas de IT e do nosso gabinete de crise, que têm de fazer esse levantamento. A comunicação, neste caso, atua sempre com dados que nos são fornecidos pelos nossos departamentos. Portanto, houve uma primeira fase de perceber, de eles fazerem esse levantamento e, também, é preciso dar tempo ao tempo, estas coisas não se fazem numa hora. Por muita pressão mediática que haja, nós temos de ter a capacidade de aguentar e de perceber que há um trabalho técnico que leva o seu tempo. Se fosse algo planeado, não era crise. A crise é exatamente isso, é algo inusitado. Portanto, na primeira fase da crise, do ponto de vista de comunicação, há aqui duas situações. Primeiro, garantir articulação com as equipas internas e garantir que estas estão a fazer o levantamento certo daquilo que é o enquadramento do ataque, para percebermos exatamente o que é que está em causa, para podermos sugerir um planeamento de comunicação. E, ao mesmo tempo para fora, ir aguentando os *media*, ir aguentando aquilo que é a pressão mediática e explicar que estamos a atuar, passar uma mensagem de tranquilidade, passar uma mensagem de que a informação que temos, até ao momento, é parca ainda… Ou seja, uma comunicação que não alimente o pânico, uma comunicação que permita ganhar tempo, mas uma comunicação verdadeira. Isto é, no meu primeiro momento nessa situação, eu nunca disse que os dados dos clientes não estavam afetados. Eu não sabia, para quê que eu ia dizer que não havia? Depois no dia seguinte era desmentido. Portanto, na EDP – e acredito que grande parte dos meus colegas de comunicação – um dos princípios é transparência e verdade da comunicação. Isso deve ser um pilar básico daquilo que é a relação com os *media* e com todos os

nossos *stakeholders*. Como se costuma dizer, a mentira tem perna curta. Uma das minhas mais-valias é ter a confiança dos jornalistas e eles saberem que aquilo que eu digo é verdade. Portanto, se eu digo que não tenho dados, não tenho dados. Se eu digo que não há problema, eles acreditam em mim. Se eu lhes digo que não há problema e depois a seguir há, perco essa relação de confiança que tenho. Portanto, numa primeira fase, tentar conter o impacto mediático. Ao mesmo tempo, internamente, esclarecer os colaboradores sobre o que está a acontecer, porque eles leem pelas notícias e também sabem e, portanto, um dos princípios básicos é informar primeiro internamente do que externamente. Portanto, os nossos colaboradores, que são embaixadores da nossa marca, também têm amigos, também têm familiares, também leem notícias e, por isso, têm de saber o que se está a passar. Mas, ao mesmo tempo, ter cuidado, porque eu não posso dizer nada a mais internamente relativamente àquilo que digo externamente… Naturalmente, porque há fugas de informação. E depois fortíssima articulação com as equipas internas. Elas depois, sim, articulam com as entidades. Do ponto de vista de comunicação, eu e a minha equipa também articulamos com as respetivas comunicações da autoridade nacional de cibersegurança, com a polícia… Há aqui uma articulação até a pedir sugestões de melhores práticas, o que aconselham. Portanto, houve ali uma fortíssima articulação com a equipa de comunicação deles, que, diga-se de passagem, super profissional. Portanto, o primeiro embate é fazer esta articulação, dentro e fora.

Q3: Ainda tendo por base o ciberataque à EDP, quais foram as implicações decorrentes do incidente para a organização?

RC: Do ponto de vista de divulgação de informação sensível ou confidencial ou que impactasse clientes ou que impactasse o negócio, não teve implicações. Se bem me recordo, aquilo era tudo informação já desatualizada e antiga. Eles não tiveram acesso aos servidores todos, tiveram só a uma pequena parte. Portanto, desse ponto de vista não houve implicações. Eu acho que houve implicações positivas, uma que teve depois como consequência outra. Primeiro, veio alertar para a necessidade de termos sistemas robustos e com segurança. Portanto, fazer investimentos em segurança de IT é um investimento, não é um custo. Nós temos de ter as nossas redes seguras, nesta lógica de haver mais teletrabalho… Obviamente há muito mais utilização digital na nossa rede e, portanto, a nossa rede tem de estar segura a ataques externos. Por um lado, essa foi a primeira evidência. A segunda evidência que decorre dessa é continuar a investir cada vez mais na segurança da nossa rede. Às vezes as pessoas pensam: "mas para quê investir este balúrdio em segurança das redes?". Mas a verdade é que isso garante que os nossos sistemas não sejam atacados. Estou a dizer isto, mas em boa verdade a EDP sempre teve uma boa consciência disto, mas obviamente sempre que há estas situações é um momento de reforço. Portanto, eu diria que, se houve implicações, foram produtivas deste ponto de vista.

Q4: Qual considera ser a importância de as organizações apostarem na comunicação de crise numa situação de ciberataque? Ou seja, o que é que esta aposta na comunicação assegura e previne à organização, tanto a nível interno, como a nível externo.

RC: A nível interno, é importante para as pessoas saberem por nós o que se está a passar. Todos nós temos amigos e familiares e, se nós queremos que os nossos colaboradores sejam embaixadores da marca, temos de garantir que estão a par da situação para informar as pessoas. Enquanto embaixadores da marca, a comunicação interna é muito importante. E isto não deve acontecer só em situações de crise, é também válido para situações correntes, como investimentos, resultados… A nossa comunicação interna é fortíssima e, portanto, queremos mesmo que os nossos colaboradores saibam o que se está a passar de bom e de menos bom, naturalmente. No fundo, trata-se de uma questão de transparência. Para fora, a coisa muda um bocadinho de figura, temos de ter muito cuidado com o que vamos dizer, porque o atacante também está a ler notícias. Portanto, isto é mais um caso de polícia do que propriamente um caso de comunicação. Ou seja, a comunicação tem de ser usada com inteligência, para não estarmos a dar argumentos ou pistas a quem nos ataca daquilo que andamos a fazer. Portanto, muitas vezes o silêncio vale ouro e dar apenas uma mensagem de tranquilidade, que estamos a atuar… Enfim, dando passos pequeninos com informação cirúrgica, sem divulgar dados que possam permitir ao atacante tomar novas posturas, sem também espicaçar o atacante, porque se eles tiverem mesmo dados podem ficar com o orgulho mais ferido e fazer ainda pior. Portanto, para fora, eu diria que temos de ter uma comunicação muito inteligente e, como digo, articulada com as autoridades, porque eles é que são os especialistas nesta matéria. Um ciberataque é um crime muito específico e com alguma sofisticação tecnológica, em alguns casos, de redes internacionais bem montadas, com meios poderosos… Eu acho que é muito importante na comunicação haver uma articulação com as autoridades. Eu diria que é uma das principais regras. Eles é que sabem, eles é que estão habituados a isto.

Q5: Qual considera ser o papel do profissional de Relações Públicas e a sua importância numa situação de ciberataque?

RC: É muito importante. Se for uma resposta escrita, como um *press release*, podemos ser nós aqui a fazer e delinear uma estratégia com as equipas técnicas. Se for, por exemplo, ir a uma televisão ou falar para uma rádio ou dar uma entrevista… Nós na EDP, apesar de eu ser o Diretor de Comunicação, não sou eu o porta-voz, porque entendo que o porta-voz tem de ser alguém que saiba esclarecer tecnicamente. Eu, enquanto responsável de comunicação, tenho de fazer a ponte com os especialistas e depois fazer o meu trabalho de bastidores, falar com os jornalistas, sensibilizá-los para o tema… Agora, o papel do porta-voz é tão importante que ele tem de ser

capaz, nestas situações, de explicar o que é que está em causa. Primeiro, tem de ter conhecimento técnico sobre o que está em causa. Segundo, a partir do momento em que é definido como porta-voz, tem de saber falar, tem de ter técnica corporal, tem de saber projetar a voz, tem de ter *media training*. Por isso é que nós aqui identificamos um conjunto de porta-vozes por temas e depois damos formação, damos *media training*. As pessoas estão sujeitas a treinamento do ponto de vista da comunicação. E depois a postura, em situações de crise, é sempre uma postura de tranquilidade e de anti-*stress*. Não é uma postura de desvalorização da crise, mas é de "estamos a trabalhar". A verdade é que o porta-voz tem um papel fundamental, pode até destruir a imagem da empresa numa situação de crise.

Q6: Tendo por base a sua experiência pessoal, quais considera ser os desafios enfrentados pelo profissional de Relações Públicas numa situação de ciberataque?

RC: Apesar de tudo, eu acho que enfrentar metade de um país às escuras é muito mais stressante do que um ciberataque, honestamente. Digamos que um ciberataque tem um impacto diferente e exige uma gestão mais aguçada, digamos assim, de reputação, é mais reputacional. Enquanto uma crise, por exemplo, de um furacão ou de inundações que deixam metade do país às escuras é reputacional, naturalmente, mas também é prático, porque temos pessoas sem luz, com comida a estragar-se nos frigoríficos e sem acesso a televisões. Portanto, a pressão mediática, por exemplo, de um furacão ou de uma inundação é dez ou quinze vezes superior a um ciberataque. Um ciberataque é, sobretudo, reputacional. Portanto, a minha primeira intuição foi tentar perceber *asap*, nas primeiras horas, o potencial de extensão dos dados afetados e depois gerir muito bem aquilo que foi o impacto mediático nacional – que foi o meu papel. Porque numa primeira fase, o impacto foi exclusivamente nacional, mas depois, ao fim de cerca de dois dias, começaram os primeiros contactos de *media* internacional. Depois, naturalmente, há sempre aquele stress de "vocês têm 5 dias para nos pagar, se não divulgamos mais dados, agora têm 4, agora já só falta 1, atenção…". Confesso que dá algum nervosismo. Será que eles estão a fazer *bluff*? Será que eles têm mesmo mais dados? Será que se nós não pagarmos eles divulgam mesmo os dados? Mas estava fora de questão. Aliás, das primeiras decisões que foram tomadas foi não se pagar nada. Portanto, é mais esse nervosismo do que propriamente a pressão mediática, honestamente. A pressão mediática num ciberataque é muito esta coisa agora da proteção de dados. Mas digamos que é mais gestão reputacional. No fundo, é como já lhe disse, é conhecer o problema rapidamente, articular com as autoridades e gerir, numa fase inicial, os *media*. E depois é ir articulando isto tudo.

Q7: No que respeita à gestão reputacional, quais considera ser as implicações de um ciberataque para a reputação de uma organização?

RC: Ninguém gosta e nunca é bonito sair nas notícias a dizer que a EDP foi alvo de um ataque. Quer dizer que houve ali sempre alguma vulnerabilidade que foi identificada. Também lhe devo dizer que não há sistemas infalíveis. Isto é como nas nossas casas, por mais que instalemos sistemas de segurança, se eles quiserem assaltar a casa, assaltam. Quando quem quer atacar, quer mesmo, há sempre uma brecha por onde entrar. Portanto, do ponto de vista da reputação, mesmo que depois não haja mais impactos – como foi o nosso caso –, fica sempre ali uma nódoa chata. Uma vulnerabilidade que foi identificada, que foi tapada entretanto, mas provavelmente existirão outras, por muito que se invista em cibersegurança. Neste caso específico, como não houve mais impactos, digamos que ficou só essa mancha. Genericamente, um ataque mais massivo, em que haja efetivamente divulgação de dados… Obviamente demonstra que não se tratava de uma pequena vulnerabilidade, mas sim uma grande vulnerabilidade. Portanto, "eu sou cliente de uma empresa que não cuida dos meus dados" e isso, do ponto de vista reputacional, é grave. E mais grave é quando o cliente deixa de ser cliente e opta por escolher o concorrente. Portanto, no limite do limite, posso vir a perder o negócio e perder clientes. Depois, obviamente, também posso vir a perder investidores. Eu quando invisto em empresas, quero investir numa empresa que seja bem vista no mercado. Portanto, do ponto de vista de acionista, também pode ter impactos. Digamos que se for um ciberataque bem-sucedido – espero que não haja muitos –, é seta acertada na reputação da empresa, isso não tenho a menor dúvida. Mais até, do ponto de vista de reputação, do que propriamente uma inundação ou um furacão. Porque efetivamente uma inundação ou um furacão é algo que nós não controlamos. Afeta naturalmente a reputação da organização, porque os clientes ficam insatisfeitos, mas é algo que as pessoas depois, até mais friamente, compreendem. Eu estou a fazer sempre esta comparação, porque acho que são duas crises com atuações e impactos distintos. Um ciberataque, do ponto de vista da reputação, ataca no âmago da reputação, porque, apesar de ser algo que não conseguimos evitar por não haver sistemas infalíveis, conseguimos blindar muito mais do que um furacão.

Q8: Já me falou dos investidores, dos fornecedores, dos colaboradores, dos *media*… Qual considera ser a importância de todos estes *stakeholders* numa situação de ciberataque? Qual a importância de comunicar com eles e saberem efetivamente o que se está a passar?

RC: É fundamental, com todos eles. Cada um ao seu nível, com diferentes mensagens, com diferentes níveis de comunicação, com diferentes níveis de tranquilidade… Quer dizer, é fundamental. Com as autoridades, porque eles é que são os especialistas e quem nos consegue ajudar. Internamente, com os departamentos certos, porque eles é que são a fonte de informação

correta. Com os colaboradores, para saberem exatamente o que se está a passar. Com os *media*, precisamente, para os ir alimentando, porque se tivermos muito tempo calados, dá azo a que outros falem. No caso dos *media*, como já lhe expliquei, tem de ser tudo comunicado com muita inteligência, de forma cirúrgica, para não divulgar determinada informação a quem está a ler notícias. Quando há uma situação destas, muitas vezes somos inundados por meios que nunca ouvimos falar, até meios internacionais. E eu não sei se estes meios internacionais estão ao serviço do atacante. Isto é tudo lições que eu aprendi com a minha colega especialista nisso. Efetivamente, a nossa comunicação com os *media* tem de ser muito inteligente. E depois com as autoridades, com os clientes, de forma a tranquilizá-los, mantê-los ao corrente da situação. Reforço que isto foi no nosso caso, porque isto não é chapa cinco. Comunicação em nada – e muito menos em situação de crise – é chapa cinco. Por isso é que, às vezes, não devemos levar os manuais de gestão de crise à letra. O nosso manual diz-nos todos os procedimentos. Mas cada situação é uma situação diferente. E, muitas vezes, quem não trabalha em comunicação não percebe isto. Muitas vezes, para a mesma situação, com uma semana de diferença, recomendo o oposto. Porque o contexto muda, a situação evolui. Portanto, das duas uma, ou nós temos um manual de gestão de crise e quase todos os meses temos de olhar para ele, ou então é um bom guia, mas quer dizer, não pode ser levado totalmente à letra. Tem de ser levado com alguma inteligência também.

Q9: O Rui já me falou de algumas medidas, também da própria experiência que teve no ciberataque de que a EDP foi alvo. Não sei se quer acrescer mais alguma medida ou ação de comunicação que as organizações devem implementar em situação de ciberataque.

RC: Eu acho que isso vai sempre depender da extensão e da dimensão da crise. Mas há coisas que são transversais, como criar uma *newsletter* específica para clientes só para esta situação, ou criar uma secção no *site* temporária só com informações sobre o incidente, ou criar uma secção só para colaboradores na nossa *intranet* sobre esta crise. Ou seja, coisas sintetizadas e mais direcionadas, de forma temporária. Mas tem de ser feito com inteligência. Uma vez mais, depende da extensão. Nós rapidamente percebemos, com uma forte probabilidade, que o ciberataque não era extenso e que o risco de eles terem mais informação era pequeno, portanto optámos por não ser muito extensos na nossa comunicação. O que não significa ausência de comunicação. É gerir a comunicação com inteligência. São coisas diferentes. Porque há casos em que o silêncio é incompetência, mas na maior parte dos casos, felizmente, é gestão de comunicação, gestão de informação. Às vezes, o silêncio vale mais do que dez notícias. Para quem trabalha em comunicação, isto é muito importante. Aliás, acho que os manuais de crise são ótimos guias, que nos permitem arrumar a cabeça e ter uma cadeia de procedimentos. Devem até ser atualizados após cada situação de crise que enfrentamos. Contudo, como já referi, aquilo não pode ser levado tão à

letra. Por exemplo, já me aconteceu várias vezes ter um *press release* pronto para sair e, de repente, um ministro faz uma declaração e eu já não faço o *press release*. Temos de ser inteligentes e, sobretudo, temos de estar em cima da informação. As pessoas que trabalham em comunicação têm de ter apetite por informação, porque isso é que lhes permite depois fazer bons planos de comunicação, em crise ou sem ser em crise. Por exemplo, na altura do ciberataque, naturalmente, interessei-me mais pelo tema e li uma série de coisas. Mas realmente também é muito importante confiar nos nossos colegas que trabalham nessas áreas.

Q10: Por último, gostaria de saber quais considera ser os riscos e ameaças do fenómeno do ciberataque para a área das Relações Públicas.

RC: Pela experiência que tenho na EDP, eu trato o tema de um ciberataque como trato de outros temas. Eu acho que os crescentes ciberataques que tem havido trazem para a organização maiores cuidados, mas para as áreas tecnológicas de IT, de segurança e de sistemas. Isso sim. Agora do ponto de vista das Relações Públicas, é um tema que eu tenho de tratar como tenho de tratar das inundações, dos furacões, dos preços da energia… É mais uma crise que eu tenho de gerir. Agora, qual é que é a dificuldade adicional, digamos assim? É que um ciberataque não é uma coisa do nosso negócio. Diria que essa talvez possa ser a maior ameaça para a área das Relações Públicas. É um caso de polícia, sobretudo. Como já lhe disse, eu de energia falo à vontade. Agora de ciberataques e casos de polícia tenho mais dificuldade, porque não é a minha especialidade. Por isso é que recorro a quem está habituado a trabalhar nessa área.

Q11: Penso que conseguimos abordar todos os tópicos que estavam previstos inicialmente. Não sei se o Rui quer acrescentar mais alguma ideia que considere relevante e que não tenhamos abordado.

RC: Penso que não. Reforço apenas a ideia principal que agarra isto tudo: ouvir os especialistas; articulação interna muito forte; uma cuidada gestão externa. E para quem trabalha em comunicação, é importante perceber que não podemos tratar todas as crises de igual modo. Cada situação é uma situação nova. A base é a mesma: há *stakeholders* para gerir; há uma situação para analisar. Mas aquilo que é o planeamento de comunicação e a execução da comunicação tem de ser específica para cada caso. E depois ter porta-vozes muito bem trabalhados, que conheçam e saibam explicar o que está em causa. E para explicar o que está em causa, têm de ser preparados, têm de ter técnicas de comunicação, têm de saber falar, têm de saber dosear – porque quem fala muito, em comunicação, não é bom. Esse é o nosso trabalho, ter pessoas preparadas para falar, em crise ou sem ser em crise.

Apêndice 13: Entrevista Anabela Lopes Simões

Q1: Gostaria que a Anabela começasse por me falar um pouco sobre a sua experiência na área da Comunicação.

AS: A minha experiência na área da Comunicação é uma experiência de quase 3 décadas. Estou no Gabinete de Comunicação da Luís Simões há 24 anos. Eu disse que eram quase 30, mas a verdade é que nos meus primeiros 6 anos tive no departamento jurídico, que é uma fonte fundamental de cultura geral, onde aprendemos imenso. Na área da comunicação, sou sincera, gosto muito mais da comunicação interna, é muitíssimo desafiante… Mas sou a responsável pelo Gabinete de Comunicação da Luís Simões a nível ibérico e, portanto, nós é que temos a responsabilidade pela comunicação externa. Comunicação interna também, a nível mais corporativo, sempre de mão dada com a área de Recursos Humanos e damos apoio em projetos de todo o tipo de atividade. Desde que estou no gabinete de comunicação, sempre tivemos agências de comunicação a trabalhar connosco. Pelo que percebi, a sua tese de mestrado está essencialmente relacionada com crise e a verdade é que nós somos talvez pessoas de sorte e não temos tido muitas crises. Também temos gerido proativamente aquilo que poderiam ser eventuais crises e acho que tem corrido bem, mesmo a nível de redes sociais. Aproveito para lhe dizer que a cibersegurança está super na ordem do dia e a questão dos ciberataques é algo que não acontece às empresas, acontece às pessoas. Quando acontece a uma empresa, a porta de entrada está nas pessoas, não está na empresa. Portanto, acho que este é um tema muito pertinente e atual.

Q2: Gostaria que a Anabela me falasse um pouco sobre a situação de crise enfrentada pelo Grupo Luís Simões aquando o ciberataque que ocorreu no dia 7 de junho de 2023. Qual foi o modo de atuação da organização perante o incidente, sobretudo ao nível da comunicação?

AS: O ciberataque do dia 7 de junho foi uma coisa que caiu assim como uma bomba, como é óbvio. Para falarmos a nível de comunicação, temos de perceber que estamos numa área de serviços e, portanto, todos os sistemas que fazem a gestão de transporte, de logística, de armazéns, de distribuição, de preparação de encomendas… está tudo em suporte digital, como é óbvio. Por acaso, temos agora um projeto de estratégia a decorrer que tem que ver com a alteração dos sistemas de gestão de armazém e distribuição - quando eu digo transportes e distribuição, nós dividimos porque transportes são de longa distância, são os chamados camiões TIR, enquanto distribuição tem mais que ver com distâncias mais curtas e normalmente em camiões mais pequenos. E, de facto, tudo o que tinha que ver com a logística, tirando duas ou três exceções, estava ainda em sistemas com já 20 anos, ou seja, esses sistemas não foram afetados. O que é que foi afetado na área da logística? Foram afetados os armazéns automáticos, que é uma dor de cabeça

desgraçada, porque aquilo está em altura, em alta densidade e, sem sistema, não se sabe onde está a palete que tem o lote de determinado produto. Portanto, esse serviço foi um *stress*, o resto conseguiu continuar a trabalhar… não diria normalmente, porque nada foi normal naquela altura, mas noutros serviços não houve efetivamente nenhum problema. Ainda ontem ou anteontem tive a revisitar alguns ficheiros dessa altura e lembro-me que no dia 8 eu devo ter produzido comunicados diferentes para enviar a clientes, para enviar a fornecedores, para enviar a bancos, para lhes dizer: "atenção, aconteceu um problema, mas nada muda nos nossos dados". Naturalmente, aqueles que se viram mais afetados o contacto não foi só esse, como é óbvio. Isto foi tudo muito imediato, mas aqueles clientes que foram, de facto, muitíssimo afetados houve contactos pessoais. Inclusive, depois quando apareceu na *dark web*, houve reuniões concretas e houve clientes muito chatos, que não deixavam abrir nada… havia clientes que não recebiam *e-mails* nossos. Pediam para criarmos uma conta no google para receberem os nossos *e-mails*. Quando percebemos o que é que tinha sido afetado, houve um grande esforço para se conseguir chegar ao máximo possível de clientes, fornecedores, entidades oficiais - aquelas que eram necessárias. Isto aconteceu a 7 de junho, mas ainda durou. Entre ativar todos os mecanismos que tinham de ser ativados e avisar todas as entidades que tinham de ser avisadas… E entre 14 e 16 de junho, foram expedidas cartas para todos os colaboradores da Luís Simões e todos os ex-colaboradores dos quais tínhamos registo - porque quem atacou podia ter acesso aos seus dados. Foram 6 mil e tal cartas, enviadas o mais rapidamente, porque isto podia ter consequências nas famílias, embora não tenhamos tido conhecimento de nada até agora. E preparámos logo, por aqueles dias, um *statement* reativo, que não usámos. A única notícia que saiu foi, de facto, a do Expresso. Esse *statement* reativo está elaborado e vai-se atualizando, mas a agência nunca o envia a ninguém sem validar connosco primeiro. E quando apareceram aquelas perguntas do Expresso, eu perguntei-lhes logo o que é que achavam e, tendo em conta o jornalista em questão, o melhor era mesmo responder. Eu costumo dizer que nós temos dois tipos de informação: aquela que damos e aquela que não damos. Naturalmente, respondemos de acordo com aquilo que ele perguntava e não acho que tenha corrido mal, porque estávamos super atentos ao resultado. Foi a única notícia que saiu. Achei que quando aquela saísse, mais iriam aparecer, mas não apareceram. O que lhe vou dizer não divulgamos a ninguém, mas claro que houve pedidos de resgate, aos quais nós não respondemos, como é óbvio. Quando acedemos a um pedido de resgate estamos a criar uma fonte de rendimento, a aumentar o risco e eles percebem que vale a pena.

Q3: O ciberataque provocou implicações à organização a longo prazo?

AS: A longo prazo, eu creio que não. As implicações que tem a longo prazo são implicações muitíssimo positivas, na minha opinião. Aliás, nas primeiras reuniões do comitê de crise, em que

estava toda a gente super cansada já, eu lembro-me que na segunda ou terceira reunião eu disse: "pessoal, vamos lá ver, vocês lembram-se do covid? Eram precisos milhões em consultoria, milhões em tudo e mais alguma coisa para nos porem a trabalhar em casa, para pôr os miúdos a ter aulas em casa e, num espaço curto de dias, aconteceu e agora já nem sabemos viver de outra maneira. Vai ser duro, mas vamos aprender com isto". Neste momento, por exemplo, temos em curso um programa de formação em cibersegurança. Uma coisa ligeira no formato, em que são feitos simulacros de *phishing* com alguma regularidade, para tentar perceber qual é a evolução… Em que vamos dar formação em vídeo, uns mais interativos do que outros. E isto serve à empresa, como é óbvio, mas serve sobretudo aos colaboradores. Como eu dizia, os ciberataques são feitos a pessoas. É preciso haver uma pessoa que deixe um bocadinho da janela aberta para o atacante conseguir entrar. Portanto, isto é algo que nos beneficia a todos individualmente. A minha leitura disto - mas eu sou uma otimista por convicção - é que as implicações a longo prazo foram positivas. Tivemos momentos muito difíceis, o mês de junho foi terrível. Por exemplo, tudo o que eram sistemas de recursos humanos, eles andaram a ver como é que faziam para conseguir pagar os ordenados às pessoas, para conseguir pagar a fornecedores… Nós temos muitos fornecedores que são empresas de transporte e que têm carros, portanto eles vivem disso. Nós tivemos de acalmar as pessoas, mandar-lhes *e-mails*. Contar o que aconteceu, mas garantir que estávamos a fazer todos os esforços para resolver a situação. A área de transportes também se viu muito afetada, porque era um sistema mais recente e eles tinham um *business continuity plan*, que tinham começado a fazer e que, durante o ciberataque, foi a forma mais fantástica de testarem o plano, foi uma situação real. Porque eles iam arrancar com o piloto e o piloto foi em real. E perceberam que tinham de ser feitos ajustes, mas estamos a falar de um *business continuity plan* que era uma folha de excel partilhada a nível hibérico. Portanto, voltamos a 20 anos atrás, em que o tráfego se geria com uns livros com mais de meio metro de largura e com um lápis de carvão e uma borracha, é quase isso… Partilhado por dezenas e dezenas de pessoas. Não foi fácil, mas conseguiu-se. Os sistemas já estão todos integrados e aquilo depois gera faturação e, naquela situação, teve de ser tudo feito à mão, mas conseguimos. Neste momento, já está tudo recuperado. Houve sistemas que optámos por não recuperar, porque percebemos que já não eram necessários e o trabalho que iríamos ter face ao benefício não compensava. Portanto, havia uma parte relacionada com recursos humanos que nós já íamos substituir o sistema, portanto apenas aceleramos a substituição do sistema e houve módulos do sistema anterior que decidimos não recuperar, porque a relação custo-benefício não era de todo favorável - sem prejuízo para os colaboradores, como é óbvio.

Q4: Qual considera ser a importância da comunicação de crise numa situação de ciberataque? Ou seja, o que assegura e o que previne à organização a aposta na comunicação, tanto a nível interno, como a nível externo.

AS: Eu sempre achei que a comunicação de crise e os planos de crise deviam estar sempre à frente. Porquê? Porque, naturalmente, nós achamos que as crises é uma coisa que só acontece aos outros. Primeiro, só a comunicação de crise não acho que resolva nada. A nossa postura e a nossa forma de ser, estar e comunicar, na minha perspetiva, tem de ser muito coerente e consistente. Porque, no dia em que há uma crise, tudo aquilo que nós dizemos as pessoas acreditam. Atenção que estou a falar de um setor extremamente conservador, eu acho que pior que isto só mesmo os bancos e as seguradoras. A área de transportes e logística, sobretudo transportes, não tem uma grande presença nas redes sociais. Se bem que agora já há mais empresas de transportes. Estou-me a lembrar, por exemplo, da LASO, que tem uma forma gira de transmitir a informação, embora seja uma empresa com outra dimensão. Mas podiam não o fazer. Há imensas empresas em Portugal, que são empresas com dimensão, e que não apostam tanto nessa comunicação. E atenção que a logística não é muito diferente. Porque é que a logística mexe? Porque aqueles que tratam da logística, também tratam da pacotaria, das entregas e, por isso, precisam de imagem para o mercado. Quando se fala de logística, as pessoas lembram-se logo da DHL, porque é a transportadora que lhes aparece à porta. E no caso da Luís Simões, muitos nem sequer sabem que também é uma empresa de logística. Portanto, é um setor mais conservador. Tanto que a nossa presença nas redes sociais é uma presença muito mais institucional. Posso dizer que, por exemplo, o *Facebook* nós utilizamos para comunicar essencialmente com os nossos motoristas. Eu sei que praticamente todos têm conta e interagem entre si… Por isso é que eu digo que a comunicação de crise, ter planos de comunicação de crise, sim, é muito importante, na mesma medida em que é difícil fazer, às vezes, a gestão de topo acreditar que isso, de facto, faz falta. Porque eles acham que isto tudo se resolve e depois ficam um bocado aborrecidos quando pedimos para não cederem à tentação de responder a tudo durante uma crise. De facto, é muito difícil fazer acreditar para cima, até porque as pessoas acham sempre que se pode responder qualquer coisa e não pode ser assim. Portanto, voltando à sua questão, é importante os *stakeholders* estarem informados. Mas temos de ver isto numa dupla perspetiva. Sim, têm de estar informados, mas por outro lado temos de ver o que é que dizemos, como é que dizemos e a quem é que dizemos para não gerar o pânico. Neste caso, das 6 mil e tal cartas que enviamos, cerca de 2600 eram colaboradores atuais, o que quer dizer que estes têm algum vínculo. Em contrapartida, houve ex-colaboradores a questionar a situação. Até porque tínhamos o canal da linha de ética aberto para responder a este tipo de questão - mas, atenção, que também não foram muitos. Portanto, é importante que as pessoas saibam, nomeadamente se têm

alguma implicação ou se podem de alguma forma ser implicadas. Sou a máxima defensora disso. Informar, sobretudo, clientes e fornecedores. Porque é assim, as pessoas têm de saber. Se as pessoas não sabem é logo um problema e começam a perder a confiança em nós. Quando se trata de clientes, é informar o cliente e procurar uma solução para entregar o serviço, porque no momento a capacidade está reduzida em *x*, nomeadamente nos sítios onde tínhamos armazéns automáticos. Normalmente, no caso dos clientes, estamos muito mais atentos e muito mais preocupados. Mas os restantes *stakeholders* também é muito importante informar. Nós estávamos lá, por isso é que no comitê de crise estava eu e estava o Diretor de Recursos Humanos. Tivemos sempre ali a contrabalançar o que é que era importante as pessoas saberem, de que forma, com que regularidade… Exatamente porque as pessoas têm de saber alguma coisa, têm de saber que algo se está a passar, porque houve pessoas que ficaram sem sistema no seu posto de trabalho. Mas também não gerar o pânico, porque depois as pessoas quando não sabem as coisas atendem uma chamada, dizem três disparates e depois esses disparates propagam-se muito mais rápido do que se propaga a verdadeira informação.

Q5: Qual considera ser o papel do profissional de Relações Públicas numa situação de ciberataque?

AS: Vou falar um bocadinho da minha experiência neste caso específico e noutras situações também. Normalmente, peço que me passem a informação global do que se está a passar. Às vezes eu não sei - e nomeadamente no caso do ciberataque - coisas que são muito técnicas e, portanto, peço que me passem a informação dos tópicos mais relevantes e em que é que isso impacta o quê e quem. E depois, normalmente, elaboro as comunicações, sendo que, no meu caso, tenho de elaborar em dois ou três idiomas: português, espanhol e inglês. Sempre em português e espanhol, em inglês só às vezes. Depois servir ali um bocadinho de polícia, para as pessoas não andarem feitas tontas a mandar *e-mails* para trás e para a frente. No fundo é um bocado isto, manter transparência e consistência na comunicação para, quando dissermos alguma coisa, as pessoas acreditarem e confiarem em nós. Tenho muito por hábito e acho que é muito didático ilustrar com exemplos, com bonecos quando tenho de passar alguma informação. Por exemplo, neste momento, temos não sei quantos projetos em curso, nomeadamente este do programa de cibersegurança, em que temos um símbolo para o projeto, em que damos algum aspeto gráfico e eu acho que isso é super importante.

Q6: Podendo tomar como base a sua experiência pessoal, quais considera serem os desafios enfrentados pelo profissional de Relações Públicas numa situação de ciberataque?

AS: Em primeiro lugar, como sou escuteira, eu estou sempre alerta para servir. E, portanto, durmo mesmo com o telemóvel à cabeceira e, naturalmente, quando sou chamada a intervir, seja em que situação for, estou de facto alerta. Eu acho que o maior desafio numa situação de crise - e não apenas ciberataque - é conseguirmos manter a sanidade mental. Já tivemos situações potenciais de crise, em que me queriam mandar para o local, seja para Barcelona, para onde fosse. Mas eu dizia sempre que precisava de ter tranquilidade, porque se não só via aquilo que todos viam. Portanto, no fundo acho que é um bocado isso, acho que temos de nos manter informados com informação de qualidade… Ou seja, há pessoas típicas em todas as organizações que dizem só aquilo que acham que tem de dizer. Isso não pode funcionar assim. Eu, inclusive, tenho um compromisso internamente - e isto demorou-me anos a conseguir - que é darem-me toda a informação. Da minha parte, não sai informação para a rua sem ser aprovada pelo Diretor-Geral e pelo administrador da área. Mas eu preciso de perceber os contornos todos. E no fundo é isto, é termos informação global de qualidade, mas não estar exatamente no olho do furacão, porque é muito fácil de nos envolvermos com toda a situação, seja um ciberataque, seja uma ameaça de greve, seja o que for. Portanto, acho necessário, em primeiro lugar, manter a coerência e a consistência e conseguir garantir a sanidade mental. Porque é normal que aqueles que estão a tratar de *hot issues* que, a dada altura, já não tenham essa sanidade toda. Eu achei que, neste caso, um terço da equipa de sistemas de informação - e criámos equipas multidisciplinares para várias coisas - cerca de um mês depois estava de baixa. Houve pessoas que durante três dias mal conseguiram descansar. Nós mandamo-los embora, mas eles não iam. E, mesmo quando iam para casa, eu acho que eles continuavam a trabalhar para resolver a situação.

Q7: Quais considera ser as principais medidas de comunicação a implementar numa situação de ciberataque, seja antes, durante e após o incidente?

AS: Relativamente à fase que antecede o ciberataque, é uma questão de prevenção, sem dúvida nenhuma. É alertar as pessoas e dizer-lhes que isto não é um problema das empresas, isto é algo que acontece às pessoas e, quando acontece às empresas, é por intermédio das pessoas. Isso é extremamente importante e, apesar de já termos feito com alguma regularidade, simulacros de ciberataques, o que é certo é que bastou uma pessoa. Houve ali uma falha e houve uma pessoa que clicou em algum *link* que deu acesso a alguém externo. Isto faz parte do antes e faz parte do após, que é aquela expressão conhecida "casa roubada trancas à porta". O que é normal é que depois de uma situação destas acontecer e de termos sentido todos na pele, as pessoas estão muito mais

predispostas a aprender sobre a questão. Se bem que toda a gente acha que sabe. Além disso, é muito importante, quando acontecem estas coisas, que se envolva e que se responsabilize os principais decisores. Ou seja, eu tenho uma equipa de *x* pessoas, então tenho obrigação de transmitir esta preocupação, antes de qualquer outra coisa, à minha equipa e, caso a equipa tenha hierarquias, aos respectivos descendentes. Isso eu acho super importante e acho que, de alguma forma, aconteceu no nosso caso. No caso do nosso programa de formação, é algo que vai durar meses e que vai ter uma cadência semanal ou quinzenal de conteúdo. Mas conteúdo mais curto, mais lúdico, que interessem e motivem as pessoas. Durante o ciberataque, é dar aquela informação, como eu já tenho vindo a dizer. Mas apenas a informação que seja útil às pessoas e que ajude a organização a restabelecer-se o mais rápido possível.

Q8: Qual considera ser a importância dos *stakeholders* numa situação de ciberataque?

AS: São muito importantes. No nosso caso, estamos a falar de acionistas, que não são assim tantos, porque a Luís Simões é uma empresa familiar. E, talvez também por esse motivo, isto não teve tanta repercussão nos acionistas. A família até tem um grupo no *WhatsApp*, portanto é relativamente fácil informá-los. Ou seja, foi mais ou menos pacífico. Também se fôssemos uma empresa cotada em bolsa, certamente isto teria tido uma repercussão muito maior. Depois, todos os nossos clientes, todos os nossos fornecedores… Eu creio que, de todos os que foram avisados, nós temos forma de ver na base de dados quais foram os fornecedores e clientes ativos e inativos, neste último caso ou porque foram bloqueados por alguma situação ou porque não têm atividade há mais de *x* tempo. E depois temos as associações a que pertencemos, as entidades oficiais, nomeadamente autárquicas… Eu não sei se nós informámos efetivamente todos os *stakeholders*. Tenho a certeza que informámos e que denunciámos à Polícia Judiciária e às entidades relacionadas com a proteção de dados, isso sem dúvida nenhuma. Fizemos tudo o que tínhamos de fazer e fomos atualizando. Mas informar todos os *stakeholders* não o fizemos. Fizemos apenas com aqueles que foram impactados ou poderiam ser impactados com a situação. Posso-lhe dizer também que os únicos *stakeholders* que tiveram um papel ativo na resolução da crise foram os nossos colaboradores, sem dúvida nenhuma. Houve muitos colaboradores a perder muitas noites de sono - e não me refiro apenas a nível de gestão e direção, estou a falar de operacionais no terreno, nomeadamente na área da logística. Esses foram os heróis. Claro que contratamos consultoras, contratamos serviços para nos ajudar a descobrir isto tudo… Agora os *stakeholders* que tiveram, de facto, um papel ativo foram os colaboradores da Luís Simões. E também creio que, mesmo com a ajuda externa, sem os nossos colaboradores não teríamos resolvido a situação. Não tenho dúvidas nenhumas.

Q9: Considera que um ciberataque pode ter implicações na reputação organizacional? Que tipo de implicações?

AS: Acho que sim. Acho que um ciberataque pode ter implicações graves na reputação de uma empresa. E essa também foi a razão pela qual não andamos a gritar aos ventos todos que tínhamos tido um ciberataque, como é óbvio. Como no nosso caso, quando chegam a ficheiros que estavam relacionados com os recursos humanos… Para ter uma ideia, nós trabalhamos bastante por picos de atividade. Os portugueses e os espanhóis insistem em fazer compras ao fim de semana e no final do mês, enquanto há países europeus que vão comprando coisas ao longo do mês. Portanto, isto cria picos de atividade. Depois há o Natal, o Dia dos Namorados, a *Black Friday*… E para isso é preciso ter recursos humanos. Nós não podemos ter lá pessoas paradas à espera de ter serviço para começar a trabalhar. E o que é que se faz nesses casos? Contrata-se empresas de *outsourcing* que colmatam esses picos de atividade para podermos cumprir as obrigações que temos acordadas com os nossos clientes. Portanto, acederam a esses ficheiros também, tivemos de avisar empresas de *outsourcing*, o pessoal da segurança… Claro que isto não teve grandes implicações porque é uma empresa familiar. Se fosse uma empresa cotada em bolsa, não seria igual. Trabalhamos com *ecommerce* também… Portanto, isto poderia ter tido implicações graves, mesmo a nível judicial. E, hoje em dia, os contratos com os nossos clientes têm já cláusulas de cibersegurança e um conjunto de variadíssimas coisas que não lhe passa pela cabeça. E faz sentido, claro. Que tenhamos informação até ao momento, não houve esse tipo de implicações, mas sim, se fôssemos uma empresa cotada em bolsa, teria tido um impacto mais complicado.

Q10: Por último, quais os riscos e ameaças do fenómeno de ciberataque na área das Relações Públicas? Ou seja, quais as implicações que poderá ter na atividade?

AS: Eu acho que pode ter implicações ao nível das Relações Públicas e do Marketing, no sentido em que, às vezes, queremos fazer uma coisa muito gira e temos de nos precaver o triplo das vezes para garantir que as pessoas acreditam em nós e não acham que o conteúdo que lhes estamos a enviar é *phishing*, por exemplo. Nós estamos a lançar o projeto em cibersegurança, que se chama Guardian, e decidimos que o primeiro *e-mail* iria sair do *e-mail* geral da área de sistemas de informação a dizer que, a partir de agora, vão receber *e-mails* de um novo endereço relacionado com o projeto. Isto para não haver reticências e hesitações por parte das pessoas. É normal que tenhamos que ter este cuidado, mas foi uma implicação que o ciberataque veio trazer à minha área. E claro que o contexto de incerteza de um ciberataque impacta a atividade, porque coloca em *standy* tudo o que estava previsto. E mesmo uma ou duas coisas que decidimos manter, houve colegas a telefonar e mandar e-mails a dizer que achavam que não devíamos ter mandado

determinado conteúdo. Acho que precisamos ali de um momento para a poeira assentar. Portanto, claro que acaba por ter impacto naquilo que tínhamos previsto. Atenção que nós vendemos imagem corporativa, nós não vendemos produto. Porque se nós vendêssemos o produto não podíamos parar, porque isso tinha implicações diretas nas vendas. Portanto, suspendemos, diria, quase a 100% as ações que tínhamos ao nível da área da comunicação. Eu fiquei no comitê de crise e envolvi a minha equipa o menos possível, ia-lhes dando apenas *feedback*. Mas como já lhe disse, se não for uma empresa com poucos acionistas, nomeadamente se for uma empresa cotada em bolsa, uma empresa com produto, com marcas… Isto pode ter um impacto muito mais complicado, mesmo tendo todos os planos de crise, tendo o dispositivo todo preparado. A nível de imagem corporativa no mercado, isto pode ter impactos nefastos, que não foi o nosso caso.

Apêndice 14: Grelha de codificação das entrevistas aos profissionais de Cibersegurança

1. Evolução dos ciberataques em Portugal

Subcategoria	Tipologia	Definição
Fase Experimental	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à caracterização dos ciberataques durante o período compreendido entre 1970 e 1980.
Pré-Cibercrime	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à caracterização dos ciberataques durante o período compreendido entre 1990 e 2000.
Fase de Desenvolvimento do Cibercrime	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à caracterização dos ciberataques durante o período compreendido entre 2000 e 2010.
Guerra Cibernética	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à caracterização dos ciberataques a partir de 2011.

2. Fatores que motivaram o aumento dos ciberataques desde 2020

Subcategoria	Tipologia	Definição
Pandemia de Covid-19	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à pandemia de Covid-19 como um fator que motivou o

		aumento dos ciberataques desde 2020.
Guerra Rússia-Ucrânia	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à guerra entre a Rússia e a Ucrânia como um fator que motivou o aumento dos ciberataques desde 2020.
Transformação digital	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à transformação digital, incluindo o aumento da dependência digital, como um fator que motivou o aumento dos ciberataques desde 2020.
Falta de literacia digital	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à falta de literacia digital como um fator que motivou o aumento dos ciberataques desde 2020.
Globalização	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à globalização como um fator que motivou o aumento dos ciberataques desde 2020.
Falta de investimento em cibersegurança	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à falta de investimento em cibersegurança como um fator que motivou o aumento dos ciberataques desde 2020.
Emergência de grupos profissionalizados	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à emergência de grupos profissionalizados como um fator que motivou o aumento dos ciberataques desde 2020.
Democratização de acesso a ferramentas e serviços de ciberataque	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à maior facilidade de acesso a ferramentas e serviços de ciberataque como um fator que motivou o aumento dos ciberataques desde 2020.
Conversão de crime tradicionalmente *offline* para crime *online*	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à conversão de crime tradicionalmente *offline* para crime *online* como um fator que motivou o aumento dos ciberataques desde 2020.
Fraca concorrência de	*Data driven*	Incluem-se nesta categoria todas

cibercriminosos a atuar no mercado português		as unidades de recorte que se referem à fraca concorrência de cibercriminosos a atuar no mercado português como um fator que motivou o aumento dos ciberataques desde 2020.
Tensão geopolítica entre a China e os Estados Unidos	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à tensão geopolítica entre a China e os Estados Unidos como um fator que motivou o aumento dos ciberataques desde 2020.
Emergência do *ransomware as a service*	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à emergência do *ransomware as a service* como um fator que motivou o aumento dos ciberataques desde 2020.
Aumento da inflação	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao aumento da inflação como um fator que motivou o aumento dos ciberataques desde 2020.

3. Atual panorama de ciberataques em Portugal

a) Tipos de ataque mais frequentes

Subcategoria	**Tipologia**	**Definição**
Phishing	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao *phishing* como um tipo de ataque frequente, atualmente, em Portugal.
Ransomware	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao *ransomware* como um tipo de ataque frequente, atualmente, em Portugal.
Fraude	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à fraude como um tipo de ataque frequente, atualmente, em Portugal.
Negação de serviço	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à negação de serviço como um tipo de ataque frequente, atualmente, em Portugal.

Perda de controlo	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à perda de controlo como um tipo de ataque frequente, atualmente, em Portugal.
Perda de dados	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à perda de dados como um tipo de ataque frequente, atualmente, em Portugal.
Smishing	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao *smishing* como um tipo de ataque frequente, atualmente, em Portugal.
Vishing	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao *vishing* como um tipo de ataque frequente, atualmente, em Portugal.
Brand phishing	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao *brand phishing* como um tipo de ataque frequente, atualmente, em Portugal.
Backdoor	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao *backdoor* como um tipo de ataque frequente, atualmente, em Portugal.
CEO *fraud*	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à CEO *fraud* como um tipo de ataque frequente, atualmente, em Portugal.

b) Setores de atividade mais atacados

Subcategoria	**Tipologia**	**Definição**
Saúde	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à saúde como um setor de atividade frequentemente atacado, atualmente, em Portugal.
Educação	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à educação como um setor de atividade frequentemente atacado, atualmente, em Portugal.
Infraestruturas críticas	*Concept driven*	Incluem-se nesta categoria todas

		as unidades de recorte que se referem às infraestruturas críticas como um setor de atividade frequentemente atacado, atualmente, em Portugal.
Administração pública	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à administração pública como um setor de atividade frequentemente atacado, atualmente, em Portugal.
Banca	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à banca como um setor de atividade frequentemente atacado, atualmente, em Portugal.
Corporate	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à área *corporate* como um setor de atividade frequentemente atacado, atualmente, em Portugal.
Direito	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao direito como um setor de atividade frequentemente atacado, atualmente, em Portugal.
Indústria	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à indústria como um setor de atividade frequentemente atacado, atualmente, em Portugal.
Comércio	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao comércio como um setor de atividade frequentemente atacado, atualmente, em Portugal.
Serviços digitais	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem aos serviços digitais como um setor de atividade frequentemente atacado, atualmente, em Portugal.

c) Riscos inerentes às organizações mais verificados

Subcategoria	**Tipologia**	**Definição**
Paralisação temporária de atividade	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à paralisação temporária de atividade como um risco inerente às organizações

		frequentemente verificado, atualmente, em Portugal.
Falência de empresas	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à falência de empresas como um risco inerente às organizações frequentemente verificado, atualmente, em Portugal.
Comprometimento de dados pessoais e confidenciais	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao comprometimento de dados pessoais e confidenciais como um risco inerente às organizações frequentemente verificado, atualmente, em Portugal.
Dano reputacional	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao dano reputacional como um risco inerente às organizações frequentemente verificado, atualmente, em Portugal.
Quebra financeira	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à quebra financeira como um risco inerente às organizações frequentemente verificado, atualmente, em Portugal.
Pagamento de resgate	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao pagamento de resgate como um risco inerente às organizações frequentemente verificado, atualmente, em Portugal.
Aplicação de coimas por parte dos reguladores	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à aplicação de coimas por parte dos reguladores como um risco inerente às organizações frequentemente verificado, atualmente, em Portugal.

4. Importância de uma organização segura

Subcategoria	Tipologia	Definição
Prevenir a ocorrência de ciberataques	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que é importante manter uma organização segura para prevenir a

		ocorrência de ciberataques.
Garantir a capacidade de recuperação de um incidente	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que é importante manter uma organização segura para garantir a capacidade de recuperação de um incidente.
Garantir a segurança dos *stakeholders*	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que é importante manter uma organização segura para garantir a segurança dos *stakeholders*.
Garantir a confiança do mercado	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que é importante manter uma organização segura para garantir a confiança do mercado.
Evitar disrupção de serviço	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que é importante manter uma organização segura para evitar disrupção de serviço.
Evitar quebras operacionais	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que é importante manter uma organização segura para evitar quebras operacionais.
Evitar o pagamento de multas	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que é importante manter uma organização segura para evitar o pagamento de multas.
Evitar perda reputacional	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que é importante manter uma organização segura para evitar perda reputacional.

5. Maturidade das empresas portuguesas em cibersegurança

Subcategoria	Tipologia	Definição
Aumento generalizado do grau de maturidade	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem um aumento generalizado do grau de maturidade das empresas portuguesas em cibersegurança.
Grau de maturidade ainda insuficiente	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o grau de maturidade das empresas portuguesas em

		cibersegurança ainda é insuficiente.
Grandes empresas com elevado grau de maturidade	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que as grandes empresas portuguesas têm um elevado grau de maturidade em cibersegurança.
PME's com reduzido grau de maturidade	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que as PME's portuguesas têm um reduzido grau de maturidade em cibersegurança.

6. Medidas de segurança

Subcategoria	Tipologia	Definição
Formação dos colaboradores	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à formação dos colaboradores, através de ações de sensibilização, como uma medida de segurança.
Aplicação de processos regulatórios e orientadores	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à aplicação de processos regulatórios e orientadores como uma medida de segurança.
Realização de avaliações de risco	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à realização de avaliações de risco como uma medida de segurança.
Estabelecimento de procedimentos de *backup* seguros	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao estabelecimento de procedimentos de *backup* seguros como uma medida de segurança.
Gestão de identidades e acessos	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à gestão de identidades e acessos do utilizador como uma medida de segurança.
Investimento em tecnologia	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao investimento em tecnologia como uma medida de segurança.
Monitorização de eventuais ataques ou ações de atividades de risco	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à monitorização de

		eventuais ataques ou ações de atividades de risco como uma medida de segurança.
Contratação de pessoas com formação adequada na área da cibersegurança	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à contratação de pessoas com formação adequada na área da cibersegurança como uma medida de segurança.
Definição de uma equipa de resposta a incidentes	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à definição de um equipa de resposta a incidentes como uma medida de segurança.
Definição de uma equipa de operações de segurança	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à definição de uma equipa de operações de segurança como uma medida de segurança.
Definição de um plano de resposta ao incidente	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à definição de um plano de resposta ao incidente como uma medida de segurança.
Definição de um plano de recuperação	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à definição de um plano de recuperação como uma medida de segurança.
Definição de um plano estratégico de segurança	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à definição de um plano estratégico de segurança como uma medida de segurança.
Definição da informação crítica, confidencial e pública	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à definição da informação crítica, confidencial e pública como uma medida de segurança.
Identificação de funções ou atividades críticas	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à identificação de funções ou atividades críticas como uma medida de segurança.
Segmentação das redes	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à segmentação das redes como uma medida de segurança.
Avaliação da rede convencional	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à avaliação da rede convencional como uma medida

		de segurança.
Definição de uma estratégia de testagem regular	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à definição de uma estratégia de testagem regular como uma medida de segurança.
Estabelecimento de atualizações de segurança regulares	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao estabelecimento de atualizações de segurança regulares como uma medida de segurança.
Inventariação dos ativos que constituem os sistemas de informação	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à inventariação dos ativos que constituem os sistemas de informação como uma medida de segurança.
Definição de uma política de utilização dos recursos TIC	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à definição de uma política de utilização dos recursos TIC como uma medida de segurança.
Estabelecimento de um registo histórico centralizado	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao estabelecimento de um registo histórico centralizado como uma medida de segurança.

7. Principais tendências na área da cibersegurança

Subcategoria	Tipologia	Definição
Inteligência Artificial	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à Inteligência Artificial como uma tendência na área da cibersegurança.
5G	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao 5G como uma tendência na área da cibersegurança.
Internet of Things	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à *Internet of Things* como uma tendência na área da cibersegurança.
Cloud computing	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se

		referem à *cloud computing* como uma tendência na área da cibersegurança.
Computação quântica	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à computação quântica como uma tendência na área da cibersegurança.
Edge computing	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à *edge computing* como uma tendência na área da cibersegurança.
Globalização	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à globalização como uma tendência na área da cibersegurança.

8. Principais desafios na área da cibersegurança

Subcategoria	Tipologia	Definição
Falta de cultura de cibersegurança nas organizações	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à falta de cultura de cibersegurança nas organizações como um desafio na área da cibersegurança.
Fator humano	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao fator humano como um desafio na área da cibersegurança.
Falta de recursos	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à falta de recursos como um desafio na área da cibersegurança.
Complexidade dos ciberataques	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à complexidade dos ciberataques como um desafio na área da cibersegurança.
Tecnologias emergentes	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem às tecnologias emergentes como um desafio na área da cibersegurança.
Redefinição mais sofisticada de *malwares* já existentes	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à redefinição mais

		sofisticada de *malwares* já existentes como um desafio na área da cibersegurança.
Falta de atualizações de segurança	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à falta de atualizações de segurança como um desafio na área da cibersegurança.
Falta de *security by design* nas aplicações e sistemas	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à falta de *security by design* nas aplicações e sistemas como um desafio na área da cibersegurança.
Democratização de acesso a ferramentas e serviços de ciberataque	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à democratização de acesso a ferramentas e serviços de ciberataque como um desafio na área da cibersegurança.
Dificuldade em justificar os investimentos em cibersegurança nas organizações	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à dificuldade em justificar os investimentos em cibersegurança nas organizações como um desafio na área da cibersegurança.
Migração para a *cloud*	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à migração para a *cloud* como um desafio na área da cibersegurança.
Acompanhamento da tendência regulatória da União Europeia	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao acompanhamento da tendência regulatória da União Europeia como um desafio na área da cibersegurança.

9. Futuro dos ciberataques em Portugal

Subcategoria	Tipologia	Definição
Aumento significativo do número de ciberataques	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o futuro dos ciberataques passa pelo seu aumento significativo.
Maior sofisticação	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o futuro dos ciberataques passa por uma maior sofisticação.

Maior influência das tecnologias emergentes	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o futuro dos ciberataques passa por uma maior influência das tecnologias emergentes, como 5G, IoT ou Inteligência Artificial.
Aumento da sensação de ameaça	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o futuro dos ciberataques passa pelo aumento da sensação de ameaça.
Aumento da capacidade de mitigação e recuperação de ciberataques	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o futuro dos ciberataques passa pelo aumento da capacidade de mitigação e recuperação de ciberataques por parte das organizações.
Aumento da literacia digital	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o futuro dos ciberataques passa pelo aumento da literacia digital.
Emergência das ameaças híbridas	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o futuro dos ciberataques passa pela emergência das ameaças híbridas.
Maior convergência entre ciberterrorismo e cibercrime	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o futuro dos ciberataques passa por uma maior convergência entre ciberterrorismo e cibercrime.
Emergência da ciberguerra	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o futuro dos ciberataques passa pela emergência da ciberguerra.

10. <u>Comunicação numa situação de ciberataque</u>

Embora esta não tenha sido uma categoria prevista inicialmente nos tópicos orientadores das entrevistas aos profissionais de Cibersegurança, por não se tratar da sua área de atuação, alguns entrevistados manifestaram a sua opinião relativamente ao papel da comunicação numa situação de ciberataque, maioritariamente de forma voluntária e espontânea, como consequência natural da realização de entrevistas de natureza semiestruturada. No contexto desta área, foram abordados dois assuntos fundamentais: a importância da comunicação numa situação de ciberataque e as

principais medidas de comunicação a ser implementadas pelas organizações numa situação de ciberataque.

a) Importância da comunicação

Subcategoria	Tipologia	Definição
Informar e esclarecer os *stakeholders*	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que a comunicação é importante numa situação de ciberataque para informar e esclarecer os *stakeholders*.
Garantir uma maior capacidade de recuperação do incidente	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que a comunicação é importante numa situação de ciberataque para garantir uma maior capacidade de recuperação do incidente.
Garantir a confiança dos *stakeholders*	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que a comunicação é importante numa situação de ciberataque para garantir a confiança dos *stakeholders*.
Tranquilizar os *stakeholders*	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que a comunicação é importante numa situação de ciberataque para tranquilizar os *stakeholders*.
Proteger a reputação organizacional	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que a comunicação é importante numa situação de ciberataque para proteger a reputação organizacional.
Garantir uma maior sensação de segurança aos *stakeholders*	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que a comunicação é importante numa situação de ciberataque para garantir uma maior sensação de segurança aos *stakeholders*.

b) Medidas de comunicação

Subcategoria	Tipologia	Definição
Confirmação da ocorrência do ciberataque	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à confirmação da ocorrência do ciberataque como

		uma medida de comunicação em situação de ciberataque.
Divulgação da situação às autoridades	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à divulgação da situação às autoridades como uma medida de comunicação em situação de ciberataque.
Estabelecimento de um plano de comunicação	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao estabelecimento de um plano de comunicação como uma medida de comunicação em situação de ciberataque.
Definição de um gabinete de crise	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à definição de um gabinete de crise como uma medida de comunicação em situação de ciberataque.
Comunicação, em tempo real, sobre o que está a acontecer	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à comunicação, em tempo real, sobre o que está a acontecer como uma medida de comunicação em situação de ciberataque.
Utilização de uma comunicação factual e transparente	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à utilização de uma comunicação factual e transparente como uma medida de comunicação em situação de ciberataque.
Utilização de uma comunicação cuidada	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à utilização de uma comunicação cuidada como uma medida de comunicação em situação de ciberataque.
Adoção de uma comunicação interorganizacional	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à adoção de uma comunicação interorganizacional como uma medida de comunicação em situação de ciberataque.
Divulgação de boas práticas de cibersegurança	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à divulgação de boas práticas de cibersegurança como uma medida de comunicação em situação de ciberataque.

Apêndice 15: Grelha de codificação das entrevistas aos profissionais de Relações Públicas

1. <u>Situação de crise enfrentada pela empresa alvo de um ciberataque</u>

a) Modo de atuação

Subcategoria	Tipologia	Definição
Informar as autoridades sobre a ocorrência do ciberataque	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o modo de atuação da organização perante o ciberataque passou por informar as autoridades sobre a ocorrência do ciberataque.
Garantir a articulação entre os vários departamentos internos da organização	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o modo de atuação da organização perante o ciberataque passou por garantir a articulação entre os vários departamentos internos da organização.
Informar os *stakeholders* sobre o incidente	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o modo de atuação da organização perante o ciberataque passou por informar os *stakeholders* sobre o incidente.
Esclarecer os colaboradores sobre o incidente	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o modo de atuação da organização perante o ciberataque passou por esclarecer os colaboradores sobre o incidente.
Utilizar uma comunicação factual e transparente	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o modo de atuação da organização perante o ciberataque passou por utilizar uma comunicação factual e transparente.
Utilizar diferentes canais de comunicação para transmitir a mensagem	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o modo de atuação da organização perante o ciberataque passou por utilizar diferentes canais de comunicação para transmitir a mensagem.
Controlar a pressão mediática	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o modo de atuação da organização perante o ciberataque passou por controlar a pressão mediática.
Avaliar a extensão do ciberataque	*Data driven*	Incluem-se nesta categoria todas

		as unidades de recorte que referem que o modo de atuação da organização perante o ciberataque passou por avaliar a extensão do ciberataque.
Convocar reuniões com diferentes *stakeholders*	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o modo de atuação da organização perante o ciberataque passou por convocar reuniões com diferentes *stakeholders*.
Responder a entrevistas para os *media*	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o modo de atuação da organização perante o ciberataque passou por responder a entrevistas para os *media*.

b) Implicações do ciberataque para a organização

Subcategoria	Tipologia	Definição
Indisponibilidade de serviços	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à indisponibilidade de serviços como uma implicação do ciberataque para a organização.
Comprometimento de dados pessoais e confidenciais	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao comprometimento de dados pessoais e confidenciais como uma implicação do ciberataque para a organização.
Maior investimento em cibersegurança	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao maior investimento em cibersegurança como uma implicação do ciberataque para a organização.

2. <u>Importância da comunicação de crise numa situação de ciberataque</u>

Subcategoria	Tipologia	Definição
Partilhar informação	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que a comunicação de crise é importante numa situação de ciberataque para partilhar informação.
Garantir a confiança dos *stakeholders*	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem

		que a comunicação de crise é importante numa situação de ciberataque para garantir a confiança dos *stakeholders*.
Tranquilizar os *stakeholders*	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que a comunicação de crise é importante numa situação de ciberataque para tranquilizar os *stakeholders*.
Permitir que os *stakeholders* tomem medidas perante a situação	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que a comunicação de crise é importante numa situação de ciberataque para permitir que os *stakeholders* tomem medidas perante a situação.
Proteger a reputação organizacional	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que a comunicação de crise é importante numa situação de ciberataque para proteger a reputação organizacional.
Garantir o alinhamento de todos os colaboradores	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que a comunicação de crise é importante numa situação de ciberataque para garantir o alinhamento de todos os colaboradores.
Evitar a proliferação de rumores	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que a comunicação de crise é importante numa situação de ciberataque para evitar a proliferação de rumores.
Permitir à organização uma maior capacidade de recuperação do incidente	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que a comunicação de crise é importante numa situação de ciberataque para permitir à organização uma maior capacidade de recuperação do incidente.

3. Papel do profissional de Relações Públicas numa situação de ciberataque

Subcategoria	Tipologia	Definição
Assumir o controlo de todo o processo de comunicação	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o papel do profissional de Relações Públicas, numa situação

		de ciberataque, passa por assumir o controlo de todo o processo de comunicação.
Articular a comunicação com o departamento de IT	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o papel do profissional de Relações Públicas, numa situação de ciberataque, passa por articular a comunicação com o departamento de IT.
Transformar a informação em mensagens adequadas a cada público	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o papel do profissional de Relações Públicas, numa situação de ciberataque, passa por transformar a informação em mensagens adequadas a cada público.
Gerir o impacto mediático	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o papel do profissional de Relações Públicas, numa situação de ciberataque, passa por gerir o impacto mediático.
Manter a calma e tranquilizar todos os envolvidos	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o papel do profissional de Relações Públicas, numa situação de ciberataque, passa por manter a calma e tranquilizar todos os envolvidos.
Ter a capacidade de recuperar do incidente e comunicá-lo aos *stakeholders*	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que o papel do profissional de Relações Públicas, numa situação de ciberataque, passa por ter a capacidade de recuperar do incidente e comunicá-lo aos *stakeholders*.

4. Desafios enfrentados pelo profissional de Relações Públicas numa situação de ciberataque

Subcategoria	Tipologia	Definição
Tempo limitado	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao tempo limitado como um desafio enfrentado pelo profissional de Relações Públicas numa situação de ciberataque.
Cadência de informação nas primeiras horas	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se

		referem à cadência de informação nas primeiras horas como um desafio enfrentado pelo profissional de Relações Públicas numa situação de ciberataque.
Instabilidade da informação disseminada	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à instabilidade da informação disseminada como um desafio enfrentado pelo profissional de Relações Públicas numa situação de ciberataque.
Capacidade de garantir a veracidade da informação	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à capacidade de garantir a veracidade da informação como um desafio enfrentado pelo profissional de Relações Públicas numa situação de ciberataque.
Capacidade de avaliar a informação que pode ser divulgada	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à capacidade de avaliar a informação que pode ser divulgada como um desafio enfrentado pelo profissional de Relações Públicas numa situação de ciberataque.
Instabilidade da situação	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à instabilidade da situação como um desafio enfrentado pelo profissional de Relações Públicas numa situação de ciberataque.
Fugas de informação	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem a fugas de informação como um desafio enfrentado pelo profissional de Relações Públicas numa situação de ciberataque.
Conhecimento técnico em cibersegurança	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao conhecimento técnico em cibersegurança como um desafio enfrentado pelo profissional de Relações Públicas numa situação de ciberataque.
Pressão mediática	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à pressão mediática como um desafio enfrentado pelo profissional de Relações Públicas numa situação de ciberataque.
Situação inicial marcada pelo desconhecido	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se

		referem à situação inicial marcada pelo desconhecido como um desafio enfrentado pelo profissional de Relações Públicas numa situação de ciberataque.
Público insciente da gravidade da situação	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao público insciente da gravidade da situação como um desafio enfrentado pelo profissional de Relações Públicas numa situação de ciberataque.
Capacidade de gerir a situação de pagamento de resgate	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à capacidade de gerir a situação de pagamento de resgate como um desafio enfrentado pelo profissional de Relações Públicas numa situação de ciberataque.
Capacidade de avaliar a extensão do ciberataque	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à capacidade de avaliar a extensão do ciberataque como um desafio enfrentado pelo profissional de Relações Públicas numa situação de ciberataque.
Capacidade de justificar a necessidade de gestão de crise à administração	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à capacidade de justificar a necessidade de gestão de crise à administração como um desafio enfrentado pelo profissional de Relações Públicas numa situação de ciberataque.
Capacidade de priorizar a saúde mental	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à capacidade de priorizar a saúde mental como um desafio enfrentado pelo profissional de Relações Públicas numa situação de ciberataque.

5. <u>Medidas de comunicação em situação de ciberataque</u>

a) Antes do ciberataque

Subcategoria	Tipologia	Definição
Divulgação de boas práticas de cibersegurança junto dos colaboradores	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à divulgação de boas práticas de cibersegurança junto dos colaboradores como uma

		medida de comunicação a implementar antes do ciberataque.
Identificação e gestão do risco	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à identificação e gestão do risco como uma medida de comunicação a implementar antes do ciberataque.
Definição de um plano de resposta ao incidente	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à definição de um plano de resposta ao incidente como uma medida de comunicação a implementar antes do ciberataque.
Realização de simulações	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à realização de simulações como uma medida de comunicação a implementar antes do ciberataque.
Mapeamento de *stakeholders*	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao mapeamento de *stakeholders* como uma medida de comunicação a implementar antes do ciberataque.
Formação de porta-vozes	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à formação de porta-vozes como uma medida de comunicação a implementar antes do ciberataque.
Execução de um exemplar impresso do manual de crise	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à execução de um exemplar impresso do manual de crise como uma medida de comunicação a implementar antes do ciberataque.

b) Durante o ciberataque

Subcategoria	**Tipologia**	**Definição**
Confirmação da ocorrência do ciberataque	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à confirmação da ocorrência do ciberataque como uma medida de comunicação a implementar durante o ciberataque.
Divulgação e articulação da gestão do incidente com as autoridades	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se

competentes		referem à divulgação e articulação da gestão do incidente com as autoridades competentes como uma medida de comunicação a implementar durante o ciberataque.
Estabelecimento de um plano de ação	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao estabelecimento de um plano de ação como uma medida de comunicação a implementar durante o ciberataque.
Recolha do máximo de informação possível sobre o incidente	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à recolha do máximo de informação possível sobre o incidente como uma medida de comunicação a implementar durante o ciberataque.
Comunicação, em tempo real, sobre o que está a acontecer	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à comunicação, em tempo real, sobre o que está a acontecer como uma medida de comunicação a implementar durante o ciberataque.
Utilização de uma comunicação factual, transparente e concisa	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à utilização de uma comunicação factual, transparente e concisa como uma medida de comunicação a implementar durante o ciberataque.
Utilização de uma comunicação cuidada	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à utilização de uma comunicação cuidada como uma medida de comunicação a implementar durante o ciberataque.
Manutenção dos diferentes canais de comunicação atualizados	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à manutenção dos diferentes canais de comunicação atualizados como uma medida de comunicação a implementar durante o ciberataque.
Criação de secções e materiais específicos com informação sobre o ciberataque	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à criação de secções e materiais específicos com informação sobre o incidente como uma medida de comunicação a implementar durante o ciberataque.

Realização de uma reunião do gabinete de crise	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à realização de uma reunião do gabinete de crise como uma medida de comunicação a implementar durante o ciberataque.
Desenvolvimento de um documento de Q&A sobre o ciberataque	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao desenvolvimento de um documento de Q&A sobre o ciberataque como uma medida de comunicação a implementar durante o ciberataque.

c) Após o ciberataque

Subcategoria	**Tipologia**	**Definição**
Realização de *follow-up* da situação	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à realização de *follow-up* da situação como uma medida de comunicação a implementar após o ciberataque.
Avaliação dos impactos decorrentes do ciberataque	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à avaliação dos impactos decorrentes do ciberataque como uma medida de comunicação a implementar após o ciberataque.
Atualização dos planos estratégicos	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à atualização dos planos estratégicos como uma medida de comunicação a implementar após o ciberataque.

6. Importância dos *stakeholders* em situação de ciberataque

Subcategoria	**Tipologia**	**Definição**
Auxiliar a organização na recuperação e mitigação de efeitos decorrentes do incidente	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que os *stakeholders* são importantes numa situação de ciberataque para auxiliar a organização na recuperação e mitigação de efeitos decorrentes do incidente.
Tomar as medidas necessárias de proteção e recuperação do ciberataque	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que os *stakeholders* são

		importantes numa situação de ciberataque para tomar as medidas necessárias de proteção e recuperação do ciberataque.
Assumir o papel de embaixadores da organização (no caso dos colaboradores)	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que referem que os *stakeholders* são importantes numa situação de ciberataque para assumir o papel de embaixadores da organização, no caso dos colaboradores.

7. Implicações do ciberataque na reputação organizacional

Subcategoria	Tipologia	Definição
Imagem negativa da organização	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à imagem negativa da organização como uma implicação do ciberataque na reputação organizacional.
Perda de confiança dos *stakeholders*	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à perda de confiança dos *stakeholders* como uma implicação do ciberataque na reputação organizacional.
Perda de clientes	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à perda de clientes como uma implicação do ciberataque na reputação organizacional.
Perda de investidores	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à perda de investidores como uma implicação do ciberataque na reputação organizacional.
Problemas judiciais	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem a problemas judiciais como uma implicação do ciberataque na reputação organizacional.

8. Implicações do fenómeno de ciberataque na área das Relações Públicas

Subcategoria	Tipologia	Definição
Oportunidade de aprendizagem	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à oportunidade de aprendizagem como uma implicação do fenómeno de ciberataque na área das Relações Públicas.
Dificuldade de fortalecimento da atividade	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à dificuldade de fortalecimento da atividade como uma implicação do fenómeno de ciberataque na área das Relações Públicas.
Dificuldade de reconstrução de relações com os *stakeholders*	*Concept driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem à dificuldade de reconstrução de relações com os *stakeholders* como uma implicação do fenómeno de ciberataque na área das Relações Públicas.
Contexto de rapidez	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao contexto de rapidez como uma implicação do fenómeno de ciberataque na área das Relações Públicas.
Maior cuidado no estabelecimento da comunicação	*Data driven*	Incluem-se nesta categoria todas as unidades de recorte que se referem ao maior cuidado no estabelecimento da comunicação como uma implicação do fenómeno de ciberataque na área das Relações Públicas.

Apêndice 16: Proposta de Guia de Boas Práticas de Prevenção e Resposta a um Ciberataque

GUIA DE BOAS PRÁTICAS EM SITUAÇÃO DE CIBERATAQUE

COMO PREVENIR E RESPONDER AO INCIDENTE

Sara Antunes
Escola Superior de Comunicação Social
Mestrado em Gestão Estratégica das Relações Públicas

ÍNDICE

INTRODUÇÃO

O crescente aumento das ciberameaças, nos últimos anos, tem provocado inúmeros desafios às organizações, sobretudo no que se refere à proteção dos seus sistemas de informação e à capacidade de recuperar de um ciberataque. As organizações estão cada vez mais expostas, em resultado do avanço tecnológico e da sofisticação das técnicas e ferramentas utilizadas nos ciberataques, provocando uma sensação de ameaça e incerteza cada vez maior.

Como devo proteger a minha organização? Como devo reagir perante um ciberataque? De que forma consigo proteger os meus stakeholders? Como posso assegurar a reputação da minha organização após ter sido alvo de um ciberataque?

Estas são algumas dúvidas recorrentes que as organizações enfrentam num contexto marcado pela imprevisibilidade e constante mutação tão características de um ciberataque.

Perante este cenário, revelou-se necessária a construção do presente guia, que reúne num único documento um conjunto de boas práticas de prevenção e resposta a um ciberataque. É urgente as organizações compreenderem a importância de estarem devidamente preparadas para a eventualidade de um ciberataque. Por mais investimento em cibersegurança que tenham, qualquer organização está sujeita a sofrer um ciberataque. Vivemos numa fase em que a questão não é saber se vamos ser atacados, mas quando!

Neste sentido, procurou-se averiguar a perspetiva de diferentes profissionais e especialistas relativamente à importância da prevenção e resposta a um ciberataque, bem como acerca das principais medidas e ações a implementar pelas organizações num incidente deste tipo. O cruzamento dos dados recolhidos nas entrevistas com informação teórica resultou na construção do presente guia de boas práticas.

O guia destina-se a todos os estudantes, profissionais ou interessados no tema da prevenção e resposta a um ciberataque. Tendo por base o estudo particular do contexto português, o guia está, essencialmente, desenvolvido para aplicação nas organizações portuguesas que pretendem prevenir e preparar a resposta a um eventual ciberataque.

DEFINIÇÃO DE CONCEITOS

Ciberespaço - *Ambiente totalmente virtual, no qual ocorre troca de informação e comunicação tendo por base uma plataforma comum de partilha de ideias, serviços e relações, não existindo qualquer fronteira física ou política* (Goutam, 2015)

Ciberataque - *Ações deliberadas contra dados, software ou hardware em sistemas ou redes informáticas, com o intuito de destruir, perturbar, degradar ou negar o acesso ao utilizador* (Denning & Denning, 2010)

Cibersegurança - *A abordagem e as ações associadas aos processos de gestão dos riscos de segurança seguidos pelas organizações e estados para proteger a confidencialidade, integridade e disponibilidade dos dados e bens utilizados no ciberespaço. O conceito inclui diretrizes, políticas e coleções de salvaguardas, tecnologias, ferramentas e formação para proporcionar a melhor proteção para o estado do ambiente cibernético e dos seus utilizadores* (Schatz *et al.*, 2017)

Crise - *Perceção de violação das expectativas dos stakeholders, que pode resultar em consequências negativas para os stakeholders e/ou para a organização* (Coombs, 1999)

Gestão de crise - *Tomada de decisões estratégicas tanto para evitar ou mitigar desenvolvimentos indesejáveis, como para proporcionar uma solução desejável em situação de crise, devendo ser um esforço contínuo por parte da organização* (Burnett, 1998)

Comunicação de crise - *Recolha, processamento e divulgação da informação necessária para enfrentar uma situação de crise. Antes da ocorrência da crise, a comunicação centra-se na recolha de informação sobre riscos de crise, tomada de decisões sobre como gerir eventuais crises e formação de pessoas que estarão envolvidas no processo de gestão de crise. Após a ocorrência da crise, a comunicação envolve a dissecação do esforço de gestão de crise, a transmissão das mudanças necessárias e o fornecimento de mensagens de acompanhamento da crise* (Coombs & Holladay, 2010)

PREVENÇÃO E RESPOSTA AO CIBERATAQUE

Um ciberataque, ao impactar o normal funcionamento de uma organização e provocar uma reação por parte dos *stakeholders*, pode potencialmente transformar-se numa crise. Qualquer situação de crise exige uma gestão de comunicação que permita não só mitigar eventuais danos decorrentes da crise, como também proteger a organização e os seus *stakeholders* - e a gestão de um ciberataque não é exceção.

Definir uma estratégia de prevenção e resposta ao ciberataque é fundamental, no sentido de orientar a organização quer no momento que antecede o incidente, como na própria gestão do ciberataque, possibilitando-lhe agir mais rapidamente e de forma mais eficaz perante uma situação de imprevisibilidade e constante mutação.

Por um lado, a prevenção constitui-se como um processo essencial no seio de qualquer organização. Estando as organizações cada vez mais expostas a violações de dados, é de extrema relevância apostarem em políticas de segurança que lhes permitam proteger os seus sistemas informáticos e, assim, garantir a confidencialidade dos seus dados e informação crítica. A implementação destas políticas é fundamental não só para prevenir a ocorrência de ciberataques, como também para garantir à organização uma maior capacidade de recuperação de um incidente e evitar disrupção de serviço.

Numa ótica de resposta ao ciberataque, é cada vez mais urgente as organizações priorizarem a fase que antecede o ciberataque, no sentido de prepararem-se devidamente para a sua ocorrência. Estando ciente de que qualquer organização se encontra exposta ao risco, a solução passa por apostar numa estratégia de preparação para que, no momento de contenção da crise, a resposta seja rápida e o mais eficaz possível. Não obstante, é inquestionável a importância da resposta à crise numa situação crítica como um ciberataque, uma vez que as ações tomadas durante o momento de crise têm um impacto direto na sua resolução e na minimização dos danos decorrentes do incidente. A fase pós-crise é igualmente fundamental por permitir à organização retirar lições que lhe serão úteis numa situação futura.

PANORAMA DE CIBERATAQUES EM PORTUGAL

Tipos de ataque mais frequentes

Atualmente, o ***ransomware*** e o ***phishing*** são os tipos de ataque mais frequentes nas organizações portuguesas. Diretamente relacionado com o *phishing*, importa destacar também a **perda de dados**, porque normalmente o que se obtém do *phishing* são credenciais que permitem o roubo de informação por terceiros.

Setores de atividade mais atacados

A **saúde** e a **educação** constituem-se como os setores de atividade mais atacados, atualmente, em Portugal, sobretudo pela sua importância e possível vulnerabilidade que, por sua vez, resultam numa maior disrupção em situação de ciberataque. De mencionar, também, a **administração pública** e a **banca** como setores de atividade em que ocorre um maior número de ciberataques em Portugal.

Riscos inerentes às organizações mais verificados

A ocorrência de um ciberataque pode produzir um conjunto de efeitos negativos sobre a organização atacada. Entre os principais riscos, destacam-se a **paralisação temporária de atividade**, o **comprometimento de dados pessoais e confidenciais**, a **quebra financeira** e o **pagamento de resgate**, em caso de *ransomware*.

TENDÊNCIAS E DESAFIOS EM CIBERSEGURANÇA

Atualmente, as organizações devem preocupar-se com um conjunto de tendências tecnológicas que têm vindo a influenciar a cibersegurança. Não obstante, esta é uma preocupação que deve ser tida em conta a longo prazo, no sentido em que o impacto das tecnologias emergentes na área da cibersegurança constitui-se igualmente como uma tendência para o futuro.

Consideram-se as seguintes tendências:

- **Inteligência Artificial**
- **Tecnologia 5G**
- ***Internet of Things***
- **Computação quântica**
- ***Cloud computing***

Diretamente relacionado com a crescente influência das tecnologias emergentes na área da cibersegurança, surge um conjunto de desafios inerentes à sua atuação. As organizações devem estar cientes destes desafios para poderem implementar políticas de segurança que ajudem a contorná-los e, assim, melhor proteger a organização.

Destacam-se os seguintes desafios:

- **Fator humano** - a grande maioria dos problemas de cibersegurança é provocada por falhas humanas;
- **Complexidade dos ciberataques** - a utilização de técnicas e ferramentas mais complexas tem tornado os ciberataques cada vez mais difíceis de defender e mitigar;
- **Falta de cultura de cibersegurança nas organizações portuguesas** - ainda se verifica uma falta de investimento em cibersegurança, seja através da implementação de tecnologia, seja na capacitação dos colaboradores;
- **Tecnologias emergentes** - a influência das tecnologias emergentes na área da cibersegurança poderá impactar em termos de deteção, prevenção e recuperação de um ciberataque.

BOAS PRÁTICAS DE CIBERSEGURANÇA

PREVENÇÃO

1 FORMAÇÃO DOS COLABORADORES EM CIBERSEGURANÇA

Sendo a maioria dos ciberataques motivados por problemas humanos, é fundamental as organizações desenvolverem **ações de formação e consciencialização em cibersegurança junto dos seus colaboradores, de forma permanente e constante**, por forma a estabelecer uma sólida cultura de cibersegurança. Estas ações devem ser desenvolvidas através de formas criativas e interessantes de passar a mensagem, para que os colaboradores assimilem efetivamente a informação que lhes está a ser transmitida e compreendam o valor fundamental dos seus comportamentos e ações para a proteção de toda a organização. Propõe-se a realização destas ações, no mínimo, uma vez por ano.

2 INVESTIMENTO EM TECNOLOGIA E CONTROLOS DE SEGURANÇA

Investir em estruturas tecnológicas e controlos de segurança permite prevenir a ocorrência de ciberataques, reduzir eventuais danos decorrentes do incidente e recuperar de forma mais eficaz. As organizações devem proteger as suas redes, através de:

- Utilização de computadores e dispositivos encriptados;
- Implementação de ferramentas de segurança, como *firewalls*, VPNs e antivírus;
- Estabelecimento de procedimentos de *backup* seguros;
- Criação de uma *cloud* interna à organização;
- Implementação de políticas de segurança, como soluções anti-*phishing* ou anti-*ransomware* que permitem identificar comportamentos suspeitos;
- Estabelecimento de atualizações de segurança regulares; entre outras medidas.

3 GESTÃO DE IDENTIDADES E ACESSOS

A implementação de uma política de gestão de identidades e acessos permite à organização proteger não só os seus recursos, como também os seus colaboradores. As organizações devem, por um lado, proteger o acesso aos sistemas através da **definição de *passwords* fortes e seguras**, procurando alterá-las frequentemente e rever as soluções de acesso remoto. Adicionalmente, deve-se **ativar o múltiplo fator de autenticação**, para confirmar a identidade do utilizador e evitar acessos indevidos por parte de terceiros.

PREVENÇÃO

4 AVALIAÇÃO DO RISCO E MONITORIZAÇÃO DE ATAQUES

A realização de avaliações de risco é fundamental para **identificar os riscos a que a organização poderá estar exposta** e, posteriormente, conseguir detê-los. Além de uma identificação clara do risco, **é necessário quantificá-lo**, para poder justificar à organização todos os investimentos realizados em cibersegurança. Como consequência direta, a identificação dos riscos permite à organização **monitorizar eventuais ataques ou ações de atividades de risco** e, assim, melhor preparar-se para a eventualidade de ocorrência de um ciberataque.

5 DEFINIÇÃO DE PLANOS ESTRATÉGICOS

Numa primeira instância, é necessário **definir um plano estratégico de segurança** assente em políticas de segurança e na definição de uma equipa de operações de segurança, com papéis e responsabilidades bem delimitadas. Posteriormente, revela-se fundamental a **definição de planos de recuperação, como sendo o *disaster recovery plan* e o *business continuity plan***, igualmente assentes na definição de políticas de recuperação do incidente e de continuidade do negócio e no estabelecimento de papéis e responsabilidades claras. Os planos estratégicos permitem à organização antecipar todos os passos e etapas, organizar ideias e definir ações, para que, no momento de implementação, consigam mais rápida e facilmente agir.

6 DEFINIÇÃO DE UMA ESTRATÉGIA DE TESTAGEM REGULAR

Não basta apenas as organizações investirem em tecnologia e controlos de segurança, definirem planos estratégicos e apostarem na formação dos colaboradores, é absolutamente essencial testá-los. Qualquer organização está sujeita a cometer erros e, no sentido de preveni-los, deve apostar na **realização de simulações que permitam colocar em prática os seus sistemas de segurança, os seus planos estratégicos e as aprendizagens dos seus colaboradores**. Esta é a forma mais segura de garantir uma eficaz prevenção, resposta e resolução de um ciberataque.

PREVENÇÃO

7 APLICAÇÃO DE PROCESSOS REGULATÓRIOS E ORIENTADORES

Por forma a garantir uma maior segurança das suas redes, as organizações devem aplicar processos regulatórios e orientadores, os quais sugerem um **conjunto de diretrizes a implementar nos controlos de segurança da organização**. Entre eles, destaca-se:

- *Zero Trust Network;*
- *NIST Cybersecurity Framework;*
- *Digital Operational Resilience Act;*
- *ISO 27001;*
- *PCI Compliance;*
- Lei *Sarbanes-Oxley*.

Estes processos permitem fornecer as diretrizes mais adequadas ao contexto atual em que vivemos, marcado pela constante mudança e evolução tecnológica.

8 DEFINIÇÃO DA INFORMAÇÃO E ATIVIDADES CRÍTICAS

A **definição da informação crítica, confidencial e pública** é fundamental para a organização conseguir priorizar os dados que merecem uma maior proteção e controlo de segurança e definir, inclusive, os acessos internos a essa informação. Além disso, revela-se essencial **identificar as funções ou atividades críticas** e, em função disso, avaliar os processos, sistemas de informação e tecnologias de informação que lhes estão associadas, por forma a identificar os riscos e, em caso de necessidade, atualizar os controlos de segurança.

OUTRAS MEDIDAS FUNDAMENTAIS:

- Contratação de pessoas com formação adequada na área da cibersegurança
- Segmentação e avaliação das redes
- Inventariação dos ativos que constituem os sistemas de informação
- Definição de uma política de utilização dos recursos TIC, subscrita pelos colaboradores
- Estabelecimento de um registo histórico de incidentes passados e procedimentos adotados

BOAS PRÁTICAS DE COMUNICAÇÃO

ANTES DO CIBERATAQUE

1 DEFINIÇÃO DE UM PLANO DE RESPOSTA AO INCIDENTE

Atualmente, qualquer organização está sujeita a sofrer um ciberataque, por muito investimento em cibersegurança que tenha, pelo que é fundamental antecipar a sua ocorrência e, por sua vez, **definir todos os procedimentos de resposta ao incidente**. O plano deve ser explícito no que respeita a:

- Estipulação de objetivos de comunicação;
- Definição da equipa de resposta ao incidente e respetivas responsabilidades;
- Estabelecimento de medidas e ações a implementar;
- Definição da informação que deve e pode ser divulgada;
- Definição dos meios através dos quais a informação será disseminada;
- Designação das pessoas e entidades a contactar; entre outras medidas.

A elaboração do plano beneficia a organização em termos da sua capacidade para lidar com este tipo de incidentes e agir de forma mais eficiente, devendo ser atualizado com a devida regularidade.

2 MAPEAMENTO DE *STAKEHOLDERS*

A incluir no plano de resposta ao incidente, a organização deve **mapear devidamente não só todos os *stakeholders* que pretende fazer chegar a sua mensagem, como também todos aqueles que, de alguma forma, lhe podem ser úteis neste processo de comunicação**, sejam parceiros, associações ou, inclusive, os próprios *media* - um processo que deve ser revisto e atualizado frequentemente. Este mapeamento permite à organização comunicar de forma orientada, direta e eficaz com os diferentes *stakeholders*, em função das suas características e objetivos específicos.

3 REALIZAÇÃO DE SIMULAÇÕES

Perante a imprevisibilidade de ocorrência de um ciberataque, revela-se fundamental as organizações **anteciparem o risco e realizarem simulações do incidente, através da testagem dos planos estratégicos e da capacidade das próprias pessoas agirem perante a situação**. No sentido de garantir a operacionalidade de todos os objetivos delineados no plano de resposta ao incidente, a realização de simulações permite à organização preparar-se devidamente para melhor gerir uma situação real de crise.

ANTES DO CIBERATAQUE

4 IDENTIFICAÇÃO E GESTÃO DO RISCO

Para melhor se prepararem para a eventualidade de um ciberataque, as organizações devem **identificar os riscos e ameaças à reputação organizacional e avaliar as áreas com maior vulnerabilidade face à ocorrência de um incidente cibernético**. Esta monitorização deve ser realizada de forma regular e permanente, por forma a garantir uma prevenção adequada ao contexto específico da organização.

5 FORMAÇÃO DE PORTA-VOZES

Nem sempre o profissional de Relações Públicas de uma organização é acionado como porta-voz numa situação de crise. No caso específico de um ciberataque, existe, até, uma maior probabilidade de um membro do departamento de IT assumir o papel de porta-voz, pelo facto de reunir o *know-how* e competências necessárias para esclarecer tecnicamente os *stakeholders*, no caso de uma entrevista ou conferência de imprensa. Neste caso, **a organização deve garantir uma formação de *media training***, que permita ao porta-voz saber falar, saber projetar a voz, ter técnica corporal, manter a postura, entre outras competências fundamentais ao nível da comunicação.

OUTRAS MEDIDAS FUNDAMENTAIS:

- Divulgação de boas práticas de cibersegurança junto dos colaboradores, através dos canais internos da organização - que devem estar bem estabelecidos
- Execução de, pelo menos, um exemplar impresso do manual de crise, no caso de uma falha energética comprometer o acesso ao documento digital

DURANTE O CIBERATAQUE

1 CONFIRMAÇÃO DA OCORRÊNCIA DO CIBERATAQUE

O primeiro passo, numa situação de ciberataque, passa por **reconhecer o incidente e confirmar a sua ocorrência junto dos *stakeholders***. É sabido que qualquer organização está sujeita a sofrer um ciberataque, o que significa que é preferível assumir o incidente e comunicá-lo, do que optar pelo silêncio e omitir uma situação que poderá ter graves repercussões na relação da organização com os seus *stakeholders*. Embora um ciberataque possa ter um impacto negativo na imagem da organização, o seu reconhecimento junto dos *stakeholders* e posterior gestão do incidente pode minimizar os danos reputacionais.

2 DIVULGAÇÃO E ARTICULAÇÃO COM AS AUTORIDADES

As organizações devem não só **comunicar às autoridades competentes a ocorrência do ciberataque, como também articular com estas a própria gestão do incidente**, pelo facto de terem o *know-how* e competências necessárias para saber como reagir eficazmente perante uma situação como esta. Mais do que uma violação de dados, um ciberataque constitui-se como um crime que, pela sua gravidade e complexidade, deve ser reportado às autoridades, como o Centro Nacional de Cibersegurança e a Polícia Judiciária, e gerido em articulação com as suas recomendações.

3 ESTABELECIMENTO DE UM PLANO DE AÇÃO

No momento de resposta ao ciberataque, é fundamental a organização **colocar em prática o seu plano de resposta ao incidente** - definido na fase que antecede a crise - **e transformá-lo num plano de ação, idealmente num prazo máximo de 24 horas após o incidente**. Este é o momento de implementar todas as medidas estabelecidas antes da ocorrência do ciberataque, que foram previamente testadas e revistas para garantir uma gestão eficaz do incidente, nomeadamente:

- Reunir o gabinete de crise;
- Ativar a equipa de resposta ao incidente;
- Comunicar com os *stakeholders;*
- Contactar as entidades necessárias;
- Cumprir com os objetivos de comunicação, entre outras medidas.

DURANTE O CIBERATAQUE

4 ARTICULAÇÃO COM O DEPARTAMENTO DE IT

A cibersegurança é uma área muito técnica e especializada, pelo que se revela essencial **o departamento de comunicação estar em permanente articulação com o departamento de IT durante todo o processo de gestão do ciberataque**, no sentido de apurar o estado da situação, ou seja, compreender quais os serviços e atividades que ficaram efetivamente comprometidos. Por forma a garantir a veracidade e fiabilidade de toda a informação que é transmitida, o profissional de Relações Públicas deve recolher o máximo de informação técnica possível relativa ao ciberataque e, posteriormente, transformá-la em mensagens adequadas a cada *stakeholder*.

5 COMUNICAÇÃO, EM TEMPO REAL, SOBRE OS ACONTECIMENTOS

Sendo um ciberataque uma situação tão imprevisível e mutável, é importante o profissional de Relações Públicas ir **monitorizando a situação e a sua evolução para poder informar devidamente os *stakeholders* sobre eventuais atualizações do estado da situação**. É fundamental os *stakeholders* estarem devidamente atualizados sobre a evolução da situação, porque também eles podem ter um papel ativo e auxiliar a organização na resolução do incidente.

6 COMUNICAÇÃO FACTUAL, TRANSPARENTE E CONCISA

Numa situação de crise, sobretudo num caso tão delicado como um ciberataque, é crucial as organizações utilizarem uma **comunicação factual, transparente e concisa, baseada na verdade como princípio fundamental**. A ocorrência de um ciberataque compromete, muitas vezes, dados pessoais e confidenciais de colaboradores e clientes e, por esse motivo, a organização tem o dever de agir com respeito e verdade perante a confiança depositada pelos *stakeholders* no seu trabalho. Optar pelo silêncio ou omitir informação importante pode colocar em causa a relação da organização com os seus *stakeholders*.

DURANTE O CIBERATAQUE

7 UTILIZAÇÃO DE UMA COMUNICAÇÃO CUIDADA

Nem sempre divulgar toda a informação é a solução. É um facto que as organizações devem reconhecer que foram atacadas e comunicá-lo aos *stakeholders*, mas existe informação que pode comprometer a própria resolução do incidente, pelo que as organizações devem ter a **capacidade de avaliar a informação que deve e pode ser divulgada**, ou seja, a informação que é útil aos *stakeholders* e que lhe permite restabelecer-se o mais rápido possível. Significa isto que **a comunicação tem de ser utilizada com cuidado e de forma inteligente**.

8 MANUTENÇÃO DE UMA RELAÇÃO DE CONFIANÇA COM OS *MEDIA*

Estabelecer uma relação de confiança com os *media* é fundamental em qualquer fase de vida de uma organização, muito embora a necessidade aumente num momento de pressão mediática como a ocorrência de um ciberataque. As organizações devem **beneficiar da sua relação com os *media* para fazer chegar a sua mensagem aos seus principais *stakeholders***, seja através de comunicados de imprensa, de conferências de imprensa ou de entrevistas para esclarecer e informar sobre o sucedido.

OUTRAS MEDIDAS FUNDAMENTAIS:

- Manutenção dos diferentes canais de comunicação atualizados - redes sociais, *website* e imprensa -, com mensagens consistentes entre si, embora de forma personalizada
- Criação de secções temporárias - tanto no *website*, como na *intranet* - e materiais específicos - como uma *newsletter* - com informação sobre o ciberataque
- Desenvolvimento de um documento de Q&A sobre o ciberataque
- Adoção de uma comunicação interorganizacional, por forma a partilhar informação sobre o ciberataque e respetivo processo de gestão e, assim, permitir que outras organizações se prepararem da melhor forma

APÓS O CIBERATAQUE

1 REALIZAÇÃO DE *FOLLOW-UP* DA SITUAÇÃO

O acompanhamento da situação é fundamental numa fase pós-crise. A organização deve procurar **analisar a evolução da crise**, ou seja, verificar se a situação está ultrapassada ou se ainda persistem problemas que merecem atenção e algum tipo de complemento de comunicação que ajude a ultrapassar a crise. Este exercício de acompanhamento dos acontecimentos possibilita à organização **elucidar os *stakeholders* sobre o que está a acontecer e o que ainda se encontra em processo de resolução**, numa ótica de comunicação transparente, com o intuito de garantir a sua confiança.

2 AVALIAÇÃO DOS IMPACTOS DECORRENTES DO CIBERATAQUE

Numa ótica de avaliação da crise, a organização deve **analisar os impactos e danos decorrentes do incidente, seja ao nível das políticas de segurança, seja ao nível da reputação organizacional**. Esta avaliação implica compreender efetivamente o que provocou a crise, como se procedeu a resolução do problema e o que poderia ter sido feito de forma diferente, reunindo um conjunto de lições aprendidas na presente situação de crise que permitam à organização, num futuro ciberataque, mitigar os ricos, preparar-se da melhor forma e garantir uma eficaz gestão da crise.

3 ATUALIZAÇÃO DOS PLANOS ESTRATÉGICOS

Após o acompanhamento da situação e consequente avaliação dos impactos decorrentes do ciberataque, revela-se essencial a organização **atualizar os seus planos estratégicos**. Sendo os planos estratégicos importantes guias no processo de gestão de crise, é fundamental **atualizá-los com as lições aprendidas durante o ciberataque** para que, numa próxima vez, se apliquem as melhores estratégias de prevenção e resposta ao ciberataque de forma rápida e eficaz.

APÓS O CIBERATAQUE

OUTRAS MEDIDAS FUNDAMENTAIS:

- Avaliação e revisão da reputação organizacional pós-incidente
- Gestão de reputação através das redes sociais
- Criação de uma incidência de FAQs no *website*, para esclarecimento de eventuais dúvidas sobre o ciberataque
- Publicação de diretrizes a nível interno, por forma a garantir a divulgação correta de todas as informações sobre o ciberataque
- Monitorização e revisão dos riscos aos quais a organização se encontra exposta

NOTAS FINAIS

Sendo a Cibersegurança uma preocupação atual nas organizações, sobretudo pelo aumento significativo do número de ciberataques, e verificando-se uma lacuna na literatura portuguesa no que respeita ao estudo da comunicação de crise em contexto de ciberataque, o presente guia constitui-se como uma mais valia não só a nível académico, como também a nível organizacional.

Com a elaboração deste guia, espera-se um maior debate em torno da importância de as organizações portuguesas não só protegerem os seus sistemas, como também preparem-se para a eventualidade de um ciberataque. Os resultados evidenciaram que é possível ser alvo de um ciberataque e, ainda assim, recuperar do incidente com o mínimo de danos possíveis e manter a reputação organizacional.

Embora tenha sido construído com base em evidências teóricas e em perspectivas defendidas por profissionais e especialistas da área, importa realçar que o presente guia de boas práticas pretende apenas oferecer orientações genéricas e servir de inspiração a todos os interessados no tema em questão.