INSTITUTO POLITÉCNICO DE LISBOA
INSTITUTO SUPERIOR DE CONTABILIDADE
E ADMINISTRAÇÃO DE LISBOA

DISSERTAÇÃO DE MESTRADO

A NOVA TECNOLOGIA 5G E A CIBERSEGURANÇA – PERCEÇÃO DOS IMPACTOS NAS ORGANIZAÇÕES E DOS DESAFIOS PARA OS AUDITORES

João Pedro Carvalhosa Pereira

Mestrado em Auditoria

Orientador: Professor Doutor Fernando J. L. Rodrigues

Diretor de Curso: Mestre Gabriel Correia Alves

Lisboa, abril de 2022

INSTITUTO POLITÉCNICO DE LISBOA
INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DE LISBOA

A NOVA TECNOLOGIA 5G E A CIBERSEGURANÇA – PERCEÇÃO DOS IMPACTOS NAS ORGANIZAÇÕES E DOS DESAFIOS PARA OS AUDITORES

João Pedro Carvalhosa Pereira - N. º 20180095

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Lisboa para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Auditoria, realizada sob a orientação científica do Professor Doutor Fernando J L Rodrigues, Docente de Carreira integrado na Área Científica de Informática.

Constituição do júri:

Presidente - Professor Especialista Fernando Carvalho

Arguente – Professora Especialista Ana Marinho Pires

Vogal - Professor Doutor Fernando J L Rodrigues

Lisboa, abril de 2022

Declaro ser o autor desta dissertação, que constitui um trabalho original e inédito, que nunca foi submetido (no seu todo ou qualquer das suas partes) a outra instituição de ensino superior para a obtenção de um grau académico ou outra habilitação. Atesto ainda que todas as citações estão devidamente identificadas.

Mais acrescento que tenho consciência de que o plágio – a utilização de elementos alheios sem referência ao seu autor – constitui falta de ética, que poderá resultar na anulação da presente dissertação.

Dedicatória

Aos meus pais e à minha tia Glória Carvalhosa que me apoiam em todos os meus objetivos e que estão sempre presentes em todos os momentos importantes.

Agradecimentos

Em primeiro lugar, quero agradecer ao meu orientador, o Professor Doutor Fernando Rodrigues, por todo o seu tempo despendido, por todos os contactos e saber na área em questão, pela paciência no cumprimento dos prazos ou na falta deles e todas as orientações e conselhos imprescindíveis para a conclusão deste projeto.

Em segundo lugar, mas não menos importante, à minha família, pelo apoio incondicional e permanente, por me terem dado todas as bases e todas as ferramentas que me permitiram chegar até aqui, por nunca desistirem de mim e não me deixarem desistir dos meus sonhos e objetivos, mesmo quando parecem impossíveis ou inalcançáveis.

Por fim, aos meus amigos, por toda a paciência e compreensão, pela ausência e falta de tempo destes últimos anos e por todo o apoio e acompanhamento no final de mais uma etapa.

A todos o meu enorme e sincero Muito Obrigado!

Resumo

A Internet tem revelado ser, ao longo dos anos, uma extensão da vida humana.

A rede de comunicações móveis que gradualmente vem a desenvolver-se, está atualmente a ingressar na quinta geração, a denominada rede 5G, que possibilitará a conexão de novos aparelhos com a Internet e de estes se conectarem entre si.

O presente projeto pretende desenvolver, investigar e alertar para a pertinência, os impactos e riscos inerentes à atividade da auditoria nas redes 5G, tendo como foco o abrupto aparecimento de novas ameaças cibernéticas, o crescente roubo de informações e dados e a necessidade de o papel da auditoria passar a ser cada vez mais de acompanhamento e aconselhamento relativamente a estas novas temáticas.

No decorrer da dissertação é possível cotejar as respostas de acordo com o tema principal de investigação que é o seguinte: Estará a auditoria pronta para a implementação do 5G e para as mudanças que daí possam advir?

O avanço da tecnologia para além de trazer novos métodos e novas metodologias para a área da auditoria, tem trazido também alguns obstáculos e dificuldades para a atividade.

Revela-se por isso fundamental estabelecer e evidenciar a relevância da Auditoria aos Sistemas de Informação (ASI) e o impacto que esta pode gerar nas organizações, inseridas nas áreas de negócio associadas às redes móveis, bem como, estabelecer e interpretar de que modo podem as empresas estabelecer políticas de conformidade e minimizar os riscos intrínsecos às suas atividades através da Cibersegurança, possibilitando às empresas acrescentar valor a todos os seus intervenientes.

Em suma, o sistema 5G é uma temática ainda muito recente e com a existência de inúmeras incógnitas para a comunidade em geral. Assim, a área do 5G e da auditoria ainda não carece de grande acoplagem não sendo possível através da presente dissertação apresentar qualquer tipo de conclusão empírica relacionada com estas duas áreas.

Deste modo, relevam-se "Considerações Finais" em resultado da investigação realizada.

Palavras-Chave: Redes Móveis, 5G, Cibersegurança, ASI, RGPD, Auditoria ao 5G

Abstract

Over the years, the internet has proved to be an extension of human life.

The mobile communications network, which is gradually developing, is currently entering the fifth generation, the so-called 5G network, which will enable new devices to connect to the Internet and to connect to each other.

This project aims to develop, investigate, and alert to the pertinence, the impacts and risks inherent to the auditing activity in the 5G networks, focusing on the abrupt appearance of new cyber-threats, the growing theft of information and data and the need for the auditing role to become more and more of monitoring and advising regarding these new themes.

During the dissertation, it is possible to compare the answers according to the main research theme, which is the following: Is the audit ready for the implementation of 5G and the changes that may arise from it?

The advancement of technology has not only brought new methods and new methodologies to the audit field, but it has also brought some obstacles and difficulties to the activity.

It is therefore essential to establish and highlight the relevance of Information Systems Auditing (ISA) and the impact it may have on organizations in the business areas associated with mobile networks, as well as establish and interpret how companies can establish compliance policies and minimize the risks intrinsic to their activities through cybersecurity, enabling companies to add value to all their stakeholders.

In short, the 5G system is still a very recent theme with numerous unknowns for the community in general. Thus, the area of 5G and auditing still lacks a great deal of coupling, and it is not possible through this dissertation to present any type of empirical conclusion related to these two areas.

In this way, "Final Considerations" are relevant because of the research carried out.

Keywords: *Mobile Networks, 5G, Cybersecurity, Computer Audit, GDPR, 5G Audit*

Índice

Índice de Tabelas

Índice de Figuras

Acrónimos e Abreviaturas

1G – Primeira Geração;

2G – Segunda Geração;

3G – Terceira Geração;

4G – Quarta Geração;

5G – Quinta Geração;

ACL – *Access Control Lists;*

AE – Auditoria Externa/Auditor Externo;

AI – Auditoria Interna/Auditor Interno;

AICPA – *American Institute of Certified Public Accountants;*

AIS – *Audit of Information Systems;*

ASI – Auditoria a Sistemas de Informação;

ANACOM – Autoridade Nacional de comunicações;

ASITA – Auditoria aos Sistemas de Informação e Tecnologias Aplicadas;

BYOD – *Bring Your Own Device;*

CAM – Controlo de Acesso aos Media;

CNCS – Centro Nacional de Cibersegurança;

CNPD – Comissão Nacional de Proteção de Dados;

COSO – *Committee of Sponsoring Organizations of the Treadway Commission;*

CRM – *Customer Relationship Management;*

CSC – Código das Sociedades Comerciais;

CSIRT – *Computer Security Incident Response Team;*

DGS – Direção Geral da Saúde;

DoS – *Denial of Service;*

DRA – Normas Técnicas de Revisão/Auditoria;

EDGE – *Enhanced Data rates for GSM Evolution;*

ePR – *ePrivacy;*

ERP – *Enterprise Resource Planning;*

EUA – Estados Unidos da América;

E-commerce – Comércio Eletrónico;

E-mail – Correio Eletrónico;

FIL – Feira Internacional de Lisboa;

Gbps – Gigabits por Segundo;

GC – Gabinete Cibercrime;

GDPR – *General Data Protection Regulation*;

GPRS – *General Packet Radio Service;*

GSM – *Global System for Mobile communications;*

HSCSD – *High Speed Circuit-Switched Data;*

IA – Inteligência Artificial;

IDS – *Intrusion Detection Systems;*

IIA – *Institute of Internal Auditor;*

IFAC – *International Federation of Accountants*;

IoT – *Internet of Things;*

IP – Protocolo *Internet*;

IPAI – Instituto Português de Auditoria Interna;

ISACA – *Information Systems Audit and Control Association;*

ISCAL – Instituto Superior de Contabilidade e Administração de Lisboa;

ITIL – *Information Technology Infrastructure Library;*

Kbps – *Kilobyte*;

KPMG – *Klynveld Peat Marwick Gesellschaft;*

LTE – *Long Term Evolution;*

MaaS – *Malware-as-a-Service;*

Mbps – Megabit por segundo;

MIS – *Management Information System;*

MP – Ministério Público;

NIS – *Network and Information Security;*

OMS – Organização Mundial da Saúde;

OROC – Ordem dos Revisores Oficiais de Contas;

OT – *Operational Technology;*

PCAOB – *Public Company Accounting Oversight Board;*

RGPD – Regulamento Geral da Proteção de Dados;

ROC – Revisor Oficial de Contas;

SA – Sociedades Anónimas;

SaaS – *Software-as-a-Service;*

SCI – Sistema de Controlo Interno;

SCM – *Supply Chain Management;*

SI – Sistemas de Informação;

SMS – *Short Messaging Service;*

SOA – *Sarbanes-Oxley Act*;

TDT – Televisão Digital Terrestre;

TI – Tecnologias de Informação;

TIC – Tecnologias de Informação e Comunicação;

TO – Tecnologia Operacional;

UE – União Europeia;

UMTS – *Universal Mobile Telecommunications System;*

WSS – *Web Summit;*

WWW – *World Wide Web;*

XSS – *Cross-site scripting;*

Capítulo I - Introdução

O presente estudo desenvolvido no âmbito do Mestrado em Auditoria do Instituto Superior de Contabilidade e Administração de Lisboa (ISCAL), possui como tema de investigação a «**A nova tecnologia 5G e a Cibersegurança – Perceção dos impactos nas organizações e dos desafios para os auditores**». Tem como objetivo analisar, investigar e evidenciar o papel da Auditoria aos Sistemas de Informação (ASI), sobre temas como as redes móveis, com especial relevância para a rede 5G, bem como, para o estudo ao nível da segurança da informação e dos dados pessoais, sobretudo no que diz respeito à Cibersegurança[1] ao RGPD e aos riscos que estes representam para as organizações.

No decorrer da sua elaboração, pretendeu-se interpretar e desmistificar com base num conjunto estruturado de mecanismos de auditoria a adaptabilidade e a preparação da área para estes novos paradigmas através da apresentação de estudos referentes à segurança da informação, ao tratamento e gestão de dados e dos respetivos riscos no âmbito da implementação da rede 5G.

1.1 Enquadramento e pertinência do tema

Com o célere progresso das novas tecnologias interligado à necessidade de estabelecer novos e melhores métodos de comunicação foram desenvolvidas ao longo das últimas décadas novas gerações móveis capazes de dar resposta às necessidades da sociedade.

Embora a tecnologia móvel esteja de tal modo presente no dia-a-dia das gerações, sobretudo das mais jovens, que nos faça crer que as mesmas existem há séculos, foi somente há cerca de 48 anos, que um investigador da Motorola, Martin Cooper, no dia 3 de abril de 1973, realizou pela primeira vez uma chamada telefónica através de um telefone móvel.

Passados quase 10 anos surgiu em 1982 a primeira geração de redes móveis, adiante designada como 1G, que veio consentir a realização de chamadas de voz.

[1] Segundo a Resolução do Conselho de Ministros n.º 92/2019 de 5 junho, no anexo intitulado de Estratégia Nacional de Segurança do Ciberespaço 2019 -2023, no ponto 1, Valores, Definições e Princípios, Parágrafo 3, a Cibersegurança consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem.

Esta tecnologia que era totalmente analógica e incerta veio a solidificar-se ao longo dos anos e a desenvolver-se de tal modo que está, atualmente, a ser introduzida a quinta geração, a denominada rede 5G.

Passadas as décadas de 80 e 90, em que as redes móveis eram uma ferramenta acessível somente a uma classe social muito restrita, atualmente representam irreversivelmente um complemento elementar para a comunicação de qualquer cidadão.

Novos contextos exigiram novas tecnologias e por sua vez, novas gerações de redes móveis. Com o passar do tempo, as pessoas e as entidades estão cada vez mais dependentes das novas tecnologias e da utilização destas, especialmente, da tecnologia móvel. Em pouco menos de 50 anos muitos conceitos modificaram e evoluíram de tal modo que, atualmente mais de metade da população mundial transporta consigo diariamente um telemóvel.

Face à atual conjuntura tecnológica, as tecnologias móveis têm vindo gradualmente a ser desenvolvidas com o propósito de acrescentar valor para as organizações e para os seus colaboradores, culminando no tipo de tecnologia mais adotada para o alcance da persecução dos objetivos das organizações, bem como, das suas atividades e tarefas do dia-a-dia.

Nos últimos anos o impacto positivo destas tem sido de tal modo notório que permitiu o desenvolvimento, readaptação e inovação das empresas e das suas atividades. Por efeito, as mudanças instituídas nos mais diversos segmentos da sociedade e concludentemente, na vida humana, alteraram significativamente os métodos relacionais, operacionais, mas sobretudo o modo de interagir e comunicar.

Com o ingresso da rede 5G, similarmente ao já sucedido com a entrada do 4G, será instituída uma nova era, aliada à era das conexões onde as empresas passarão a ter a necessidade de criar novas ferramentas de interação e de comunicação que se irá certamente traduzir numa valiosa ferramenta de trabalho e que trará valor acrescentado para os seus negócios.

Não obstante, as organizações atravessam outros desafios para além dos intrínsecos às novas redes tecnológicas, nomeadamente no que diz respeito à segurança da informação e dos dados pessoais que estas armazenam.

Os ataques aos Sistemas de Informação (SI), começaram a surgir um pouco por todo o mundo, especialmente pelo facto da informação armazenada já não se encontrar somente num espaço exclusivo e restrito, mas sim num local *online*, designado por Ciberespaço[2].

Atualmente, não se trata somente de assegurar o correto funcionamento das atividades e serviços das organizações, mas sobretudo de salvaguardar o correto funcionamento das suas operações no que diz respeito à segurança de informação e dos dados pessoais uma vez que estes espaços são acessíveis a utilizadores capazes de comprometer a informação.

Para além da acessibilidade é preciso ter em consideração que estes espaços conferem características onde as informações podem ser recolhidas e armazenadas a partir de locais geograficamente distintos o que, devido a ambientes complexos, dificulta o controlo de acessos indesejados por parte de pessoas mal-intencionadas, os denominados *Hackers*[3].

A necessidade de implementar uma rede segura e independente que possua uma forte componente ao nível da segurança tecnológica, capaz de dar resposta a eventuais ciberataques, torna-se imprescindível para a subsistência de qualquer Organização.

Esta lacuna premissa de estudo da presente investigação, mais acentuada nas organizações que ao longo dos anos têm sido alvo de preocupantes invasões ao nível da informação e dos dados pessoais que se encontram armazenados nos sistemas tecnológicos destas, permitem auditar a ocorrência de inúmeros ataques informáticos.

Em complementaridade ao supramencionado, o presente estudo centra-se na pertinência de refletir, interpretar, estudar a evolução e adaptação do 5G e da Cibersegurança, no domínio da ASI, assim como, compreender e analisar os riscos inerentes à sua adoção e estabelecer questões pertinentes para o desenvolvimento das temáticas em estudo na presente investigação, tendo por base a segurança da informação e a proteção de dados.

[2] Segundo a Resolução do Conselho de Ministros n.º 92/2019 de 5 junho, no anexo intitulado de Estratégia Nacional de Segurança do Ciberespaço 2019 -2023, no ponto 1, Valores, Definições e Princípios, Parágrafo 3, o Ciberespaço consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação.

[3] *Hackers* - indivíduos com conhecimentos e técnicas capazes de modificar e/ou roubar informação privada armazenada em sistemas de informação.

Resumidamente pretende-se no contexto da presente investigação identificar e analisar a evolução das redes móveis, em específico, a rede 5G, bem como, clarificar o papel da auditoria, particularmente no que respeita à recolha, partilha e segurança da informação e dos respetivos dados pessoais tendo por base um estudo das temáticas envolventes com especial relevância para as vertentes científicas, sociais e profissionais.

1.2 Objeto e Objetivos

O célere crescimento do mercado atual e das novas tecnologias, quer na dimensão das empresas, quer nas atividades de negócio inerentes às redes móveis, impõe por parte das entidades competente um controlo cada vez mais rigoroso e disciplinado.

Neste sentido, torna-se essencial que a ASI adapte os seus processos e mecanismos, tente compreender a licitude de algumas práticas, como a recolha de dados e ao mesmo tempo verificar em virtude destes avanços tecnológicos, se tudo se encontra em regular conformidade com as exigências e os requisitos constantes nas normas vigentes.

O "Objeto" da presente investigação está associado ao 5G, efetivamente uma grande mudança no paradigma das empresas e das suas atividades. É irrefutável que com um mundo cada vez mais tecnológico que assiste diariamente a inúmeras transformações a todos os níveis, revela-se cada vez mais necessário que a auditoria se posicione e acompanhe tais mudanças de forma que o seu papel seja executado com toda a plenitude e conformidade, para que as modificações aos processos, aos mecanismos e às normas não ocorram tardiamente em relação às inovações da tecnologia impostas pelo 5G.

A elaboração desta dissertação tem como principais objetivos investigar e perceber o papel da auditoria relativamente a assuntos inerentes à utilização da rede móvel 5G, compreender de que forma a presença do RGPD é uma preocupação, uma vez que também foi tido em consideração. Especificamente, no que se refere à recolha de dados pessoais de forma não consentida e inconsciente por parte dos utilizadores, aferir alguns dos perigos cibernéticos associados ao uso do 5G e entender de que modo a ASI pode ajudar as entidades a prevenirem-se sobre potenciais danos colaterais próprios do emprego da tecnologia 5G.

Existem danos colaterais que são também objeto de estudo, assim como, os riscos inerentes às novas tecnologias, embora já façam parte do nosso léxico, em consequência de um acesso cada vez mais massivo à Internet, com o consequente aumento do número de utilizadores, com a necessidade de guardarem e partilharem informações em rede, o que resulta em que, a segurança do Ciberespaço tenha de passar a ser encarada pelas entidades e pelas pessoas em geral de uma maneira realmente séria.

1.3 Metodologia

Na opinião de Prodanov & Freitas (2013, p.14) a metodologia pode ser definida como:

> «[...] *a aplicação de procedimentos e técnicas que devem ser observados para a construção do conhecimento, com o propósito de comprovar a sua validade e utilidade nos diversos âmbitos da sociedade*.».

A metodologia utilizada na presente dissertação integra conhecimentos e competências adquiridas no decurso do mestrado, tendo como objetivo a apresentação de controlos de auditoria e de recomendações para a problemática da auditoria ao 5G e da Cibersegurança tendo por base um enquadramento teórico e uma revisão literária. Posteriormente, compreende também a apresentação dos resultados obtidos e das considerações finais de modo fundamentado e justificado.

A sustentação da metodologia adotada no enquadramento teórico passou por uma criteriosa recolha de elementos, realizada através do método histórico, fundamentada com legislação vigente e com informação recolhida através de livros, investigações, estudos, artigos e revistas científicas.

Na segunda parte da dissertação, foram adotados os métodos descritivo, exploratório e indutivo, através da realização de conversas informais que constituíram parte da investigação qualitativa desenvolvida na presente dissertação, com o objetivo de descrever o fenómeno do 5G, compreender as suas alterações face às anteriores versões e os seus riscos face à segurança da informação e dos dados pessoais, que culminaram na apresentação e descrição dos temas do estudo empírico, face ao contexto em que o mesmo se insere.

Na parte que diz respeito ao estudo empírico foi assumida uma metodologia maioritariamente investigacional, através de diferentes meios, mecanismos e métodos, cuja investigação pretende assim apresentar um resultado que espelhe a realidade atual e fidedigna sendo que esta não é baseada exclusivamente em casos ou situações empíricas, mas sim formulada através da utilização dos métodos relacionados com a investigação.

O sentido crítico no deparo com os casos/situações inovadoras e invulgares, passando pela participação em eventos, feiras, discussões e conversas informais sobre a temática, foi possível reunir informação e formar algumas ideias relevantes para consolidar o objeto da investigação.

Na última fase são evidenciados os temas estudados, a persecução dos objetivos, apresentadas as considerações finais e recomendações para investigações futuras. Esta fase assinala a indicação das principais reflexões e descobertas. Tem uma ligação com os temas de partida e a confirmação das mesmas.

Nada se pode concluir uma vez que a simples palavra "Conclusão" é na verdade uma dedução extraída dos resultados do trabalho realizado. Algo definitivo. Um estudo empírico nada conclui e salvo melhor opinião, apenas aponta caminhos para futuras investigações.

A opção apresentada como «Considerações Finais» indica que o resultado do trabalho de investigação possibilita reflexões, sem uma conclusão definitiva ou um resultado suscetível de revisões. Assume-se uma humildade académica que se pretende relevar e fica deste modo justificado um escrutínio público, que de acordo com as regras é importante acontecer.

1.4 Estrutura da Dissertação

O presente estudo de investigação encontra-se subdividido em cinco capítulos.

O primeiro capítulo, intitulado como «Introdução», apresenta um epítome dos elementos que se encontram implícitos no desenvolvimento da presente investigação. São evidenciados pontos essenciais ao desenvolvimento da dissertação, nomeadamente o objeto, os objetivos e a metodologia da investigação, bem como, a motivação e pertinência do tema face à conjuntura atual da nossa sociedade.

Por sua vez, o segundo capítulo «Revisão da Literatura» suporta em termos bibliográficos e investigacionais o tema da presente dissertação onde se apresentam, estão refletidas e discutidas, as principais particularidades relacionadas com a auditoria, a Cibersegurança, os SI e as mais recentes tecnologias inerentes às redes móveis em específico, o 4G e 5G, bem como, se evidenciam as suas características e contingências.

No terceiro capítulo, com o título «Enquadramento Teórico», são apresentados os temas, metodologias e os procedimentos utilizados no presente estudo que servem de base para a prossecução dos objetivos, culminando no estudo e na análise de três distintos casos que possuem como ponte de ligação as particularidades inerentes às redes móveis do 4G e do 5G, salientando a criticidade da auditoria e dos SI e evidenciando a pertinência da Cibersegurança para estes casos.

O quarto capítulo «Aplicação Prática» espelha a apresentação e interpretação dos resultados obtidos no decorrer do presente estudo, evidenciando controlos de auditoria ao nível do 5G, da cibersegurança e da proteção de dados.

Por fim, é apresentado no quarto capítulo «Considerações Finais» que, conforme já referido, ilustram um raciocínio dos principais entendimentos do que se investigou e as limitações detetadas no decurso desta dissertação, assim como, algumas propostas para investigações futuras, possíveis de desenvolvimento, enquadradas no tema apresentado.

Salvaguarda-se a inexistência de «Conclusões» que poderiam ser apresentadas, mas que apesar disso, dão lugar a “Considerações Finais”. As mesmas possibilitam uma aprofundada e necessária reflexão que se deseja lançar a todos os interessados nesta temática.

Capítulo II – Revisão da Literatura

2.1 Conceito e Evolução Histórica da Auditoria

Os serviços de auditoria têm vindo a passar, ao longo dos tempos, por dissemelhantes adversidades e significativas alterações no modo e campo de atuação.

A constante mutação da sociedade impõe que a função da auditoria tenha por base um papel decisivo no apoio às organizações, especialmente ao nível da gestão, na avaliação do sistema de controlo interno e na eficácia e eficiência das operações. Numa fase inicial, a área de trabalho da auditoria incidiu, durante muitos anos, nas contas da Administração Pública, através das civilizações como a egípcia, a grega e a romana que foram pioneiras. (Valencio e Ngueve, 2013, p. 20).

No entanto a auditoria que atualmente se desenvolve na opinião de Costa (2014), teve intento no Séc. XIX na Grã-Bretanha, como corolário das novas necessidades decorrentes da revolução industrial que foi impulsionadora no crescimento das organizações, conduzindo à concentração dos capitais, onde o propósito fundamental da auditoria consistia na verificação de fraudes na utilização dos fundos. Para a realização dessa análise, as contas auditadas eram submetidas a um exame minucioso, alicerçado na precisão aritmética e na conciliação com a anuência dada para a tutela dos fundos.

A determinação de fraude e de erros técnicos passou a ser aceite após 1884, como um propósito fundamental da auditoria. Evidenciando que a investigação do auditor por logros deveria ser incansável e constante, era solicitado aos auditores que acompanhassem as auditorias com uma agilidade plausível e que agissem de acordo com as circunstâncias. Na falta de suspeitas não lhes era imposto que investigassem a existência de fraudes, ainda assim, se esses pressupostos existissem, era-lhes proposto que as investigassem pormenorizadamente.

A partir de 1920 os auditores foram perfilhando cada vez menos responsabilidade no reconhecimento de fraudes, expondo que a prudência e o reconhecimento de fraudes eram da responsabilidade dos gestores das empresas e que o principal objetivo da auditoria era a fiabilidade dos relatórios financeiros. A previsão para a existência de fraudes presume prover a empresa de um eficiente e eficaz sistema de controlo interno.

As normas de auditoria adotadas neste intervalo de tempo foram desresponsabilizando os auditores de qualquer incumbência neste campo, que salvo melhor opinião, essencialmente eram conhecimentos de contabilidade e provas de eficiência na execução do seu trabalho.

Esta renovação nos objetivos da auditoria é fundamentada pelas mudanças socioeconómicas que surtiram nesta altura. As empresas foram progredindo não só em dimensão, mas também em complexidade, de tal modo que para submeterem as atividades dos funcionários e prevenirem, bem como, constatarem lapsos e irregularidades nos registos contabilísticos, foram produzindo e aperfeiçoando sistemas de controlo interno.

O consequente incremento de volume de transações tornou inexecutável, dentro das metas temporais e financeiras concetíveis, que os auditores certificassem todas as transações. Desta forma ao invés de dissecarem cuidadosamente cada transação, passaram a avaliar o sistema de controlo interno e a adotar a amostragem na análise dos registos contabilísticos.

Segundo Nabais (1993, p. 94) a auditoria externa consiste num:

> «(...) exame sistemático das demonstrações económicas e financeiras (Balanço Analítico, Demonstração de Resultados Líquidos, Anexo, etc.) de uma empresa e ainda dos registos e operações efetuados, com a finalidade de verificar se estão de acordo com os princípios de contabilidade geralmente aceites, com as políticas estabelecidas pela direção e com qualquer outro tipo de exigências legais ou voluntariamente aceites.»

Para Taborda (2015, p.14) «a auditoria consiste num processo de julgamento assente na recolha e análise de evidências apropriadas e suficientes e que fundamentam a opinião do auditor sobre a conformidade entre determinados procedimentos e um quadro de referência previamente definido».

Foi então no Séc. XX que se deu um impulso importante no ramo da auditoria, um século caracterizado pelo triunfo dos auditores. O entendimento dos investidores perante as empresas alterou-se, estes deixaram de estar associados às empresas de uma forma emotiva, transpondo os seus investimentos e o seu capital para sociedades cuja verosimilhança de receberem dividendos pelo investimento concretizado fosse elevado e mais estável.

Esta mudança de postura incitou alterações em relação à informação compreendida nos relatórios financeiros, sendo posteriormente ponderada como uma procedência de informação primária ao nível da tomada de decisão.

Assim sendo, os relatórios de auditoria fundamentaram-se na averiguação da credibilidade e razoabilidade da informação descrita nos relatórios financeiros, para que estes servissem como um instrumento independente e viável para a tomada de decisão.

No ponto de vista de Bedoya, Bendermacher & Craig (2016) a função de Auditoria Interna (AI) assegura clarificar o CEO, o Conselho de Administração e a gestão no que diz respeito aos potenciais riscos que possam comprometer os objetivos estratégicos de uma Organização.

A rejeição de qualquer incumbência relativa ao exercício das funções dos auditores na procura incessante de erros e fraudes passou a ser julgada de uma forma geral, na década de 60. Em objeção, normas profissionais preveniam os auditores para que na orientação da auditoria, permanecessem vigilantes à presença de fraude. Caso esta se mantivesse, o auditor deveria retificar a materialidade da fraude e emitir a sua opinião sobre os relatórios financeiros. As recomendações no seio da auditoria prosseguiram e continuam atualmente a sublinhar que o dever pela procura de erros e fraudes é da incumbência do órgão de gestão.

2.1.1 A Crise na Informação Auditada do Séc. XX ao Séc. XXI

No Séc. XX, entre os anos 80 e 90, iniciou-se uma crise de confiança nos mercados e na informação auditada incitada pelos escândalos fraudulentos das empresas nas mais distintas áreas económicas. Conturbadas foram as duas últimas décadas do Séc. XX, diversas foram as críticas publicadas sobre as empresas que executavam auditorias com o propósito de apurar responsabilidades perante as mesmas. O presidente dos Estados Unidos, George W. Bush aprovou, a 30 de julho de 2002, a lei *Sarbanes-Oxley Act* (SOA), com o propósito de restabelecer a confiança dos investidores e dinamizar o mercado de capitais em resultado de diversos escândalos em termos de capitalização bolsista dos Estados Unidos, nomeadamente o escândalo da empresa *Enron*.

A Enron era uma das maiores empresas da época que fracassou meses depois de ter recebido uma opinião limpa emitida pelos auditores (Arthur Andersen). A problemática da sociedade *Enron* tornou-se controversa devido ao facto de a mesma incentivar os seus cooperantes a investir as suas economias, ao mesmo tempo em que os colaboradores de topo transacionavam as suas posições, privilegiadas pela informação confidencial que possuíam, face à situação financeira real da empresa.

As ações de *Enron* submergiram de 90 dólares para menos de 1 dólar. Meses mais tarde a empresa de auditoria Arthur Andersen ficou afeta ao processo judicial que a *Enron* atravessava, ficando a primeira condenada pela execução de intervenções financeiras duvidosas. Complementarmente aos serviços de auditoria, a empresa prestava ainda serviços de consultoria, sendo ela própria a auditar o seu trabalho.

Para além de *Enron*, outras empresas como a *WasteManagement* (junho de 2003) e a *Sunbean* (2002) estiveram também associadas a escândalos que colocariam em causa as funções e a independência não só da Arthur Andersen, uma das mais prestigiadas empresas de auditoria, como das funções da auditoria no seu geral e dos auditores.

Paralelamente na Europa também se assistiu à insolvência de diversas empresas de grandes dimensões como a *Ahold, Parmalat* e *Vivendi*. Infelizmente muitas foram as empresas que apresentaram escândalos idênticos à de *Enron*, divulgando lacunas nas normas das *práxis* contabilísticas e de auditoria originando a implementação da Lei SOA. Um dos principais propósitos desta lei foi o de solicitar que as sociedades, cotadas nos Estados Unidos da América (EUA), reportassem sobre a eficiência e eficácia dos sistemas de controlo interno relativos ao relato financeiro. A Lei SOA inclui amplos deveres e obrigações para administradores, gestores, auditores e analistas de valores mobiliários.

O impacto que a Lei SOA teve na profissão de auditoria foi importante para ultrapassar os problemas morfológicos existentes. Uma das medidas estruturantes foi a implementação do *Public Company Accounting Oversight Board* (PCAOB), promovendo a independência dos auditores, uma entidade que possuía o dever de criar normas de auditoria, modelos morais e deontológicos que antecipassem casos de conflitos de interesses, atuando como uma entidade de supervisão. Apesar do cumprimento da SOA ser apenas obrigatório para as empresas cotadas em bolsa, as empresas não cotadas na bolsa sentiram a pressão dos mercados para cumprirem com os requisitos da SOA.

Transversalmente aos escândalos nas empresas, surgem em 2006 situações semelhantes com as instituições de crédito. Apareceu a crise do *Subprime* derivada da insolvência de diversas instituições de crédito, que disponibilizavam empréstimos hipotecários de elevado risco, após auditorias com emissão de opiniões limpas. Uma *práxis* que conduziu muitos bancos para uma posição de insolvência, que afetou drasticamente as bolsas de valores de todo o mundo.

Em 2010 a Comissão Europeia divulgou o Livro Verde que evidencia a cooperação da auditoria diante da estabilidade financeira, facultando garantias sobre a autêntica situação financeira das empresas, com a finalidade de reinstituir a confiança nos mercados, auxiliando os investidores e minimizando o risco de informação.

2.1.2 A Auditoria em Portugal – Ordem dos Revisores Oficiais de Contas (OROC)

Surgiu em 1969 pela primeira vez a obrigatoriedade de certificação legal de contas na Legislação Portuguesa, assim como, a designação de Revisor Oficial de Contas (ROC) regulado pelo Decreto-Lei n.º 49381 de 15 de novembro.

Este diploma estabeleceu a necessidade de que as Sociedades Anónimas (SA) tivessem de incorporar pelo menos um ROC no seu Conselho Fiscal ou designar um Fiscal Único e «[…] atribui aos ROC funções de interesse público no âmbito da fiscalização das contas e da gestão das sociedades anónimas, ou por quotas com conselho fiscal» (OROC (a), 2012, p. 1). Atualmente, a certificação legal das contas aplica-se não só às SA, mas também às sociedades que se encontram nas condições previstas no artigo 262.º do Código das Sociedades Comerciais (CSC).

Em Portugal, a atividade de auditoria está fundamentalmente dividida em dois grandes grupos, a Auditoria Externa (AE) e a AI fortemente sustentadas por duas instituições: a Ordem dos Revisores Oficiais de Contas (OROC), que é a base constitucional e legal e o Instituto Português de Auditoria Interna (IPAI) que procura ajudar os profissionais de AI.

Em 1972 surgiu o primeiro estatuto dos ROC, expresso no Decreto-Lei nº. 1/72, de 3 de janeiro e em 1974 onde o Governo da República Portuguesa decretou a constituição da Câmara dos Revisores Oficiais de Contas, através da Portaria nº. 83/74, de 6 de fevereiro. Mais tarde, em 1983 foram divulgadas as Normas Técnicas de Revisão Legal de Contas. Mais tarde em 1987 foi promulgado o Código de Ética e Deontologia Profissional.

No decorrer dos anos perante a necessidade de adaptação ao desenvolvimento circundante, não só a nível nacional como a nível internacional e de realizar ajustes resultantes da realização da sua prática, foram ajustados não só o estatuto dos revisores, bem como, as normas. Foi também alterado o enquadramento institucional, modificando a designação inicial de «Câmara» para Ordem, a designada OROC.

Constitui competência da Ordem segundo a alínea a) do artigo 5º do estatuto da OROC, «[e]xercer jurisdição sobre tudo o que respeite à atividade de revisão/auditoria às contas e serviços relacionados, de empresas ou de outras entidades, de acordo com as normas de auditoria em vigor». Estas normas reservam-se a preservar e clarificar uma quantidade de diretrizes relevantes para execução de trabalhos e dividem-se em normas gerais, normas de trabalho de campo e normas de relato.

Vinte anos mais tarde, a 6 de março de 1992 é instituído o IPAI uma associação profissional sem fins lucrativos que representa, a nível nacional, *The Institute of Internal Auditors* (IIA) e os auditores internos. Os principais objetivos da sua atuação passam pela defesa dos interesses dos profissionais de AI, por promover os princípios éticos no desempenho da AI e por contribuir para a formação em conhecimentos, metodologias e praticas atualizadas de modo a permitir aos seus membros uma evolução e atualização constante de conceitos.

A nível internacional, a OROC é membro efetivo da *International Federation of Accountants* (IFAC) desde 16 de novembro de 2016 e preserva ligações de grande proximidade com os organismos idênticos de outros países. É indispensável para a profissão, a união em rede a organizações internacionais para que o progresso e difusão dos aspetos técnicos possam contribuir para a sua credibilidade.

Estas instituições que envolvem os profissionais de auditoria têm como objetivo principal salvaguardar o bom nome da profissão através da realização de conferências, formações, exames e da atualização de normas internacionais e nacionais, tanto a nível técnico como a nível deontológico.

Para além destes dois organismos que conduzem boas práticas em auditoria, têm emergido cada vez mais novas configurações que atuam sob modalidades especificas. A título de exemplo, temos o caso da auditoria forense. Estas especializações emergentes podem diversificar devido à área, génese, âmbito, profundidade ou extensão dos procedimentos a aplicar.

De uma forma mais generalizada a auditoria pode ainda ser subdividida em auditoria de fonte legal quando é imposta por lei ou auditoria voluntária quando é realizada por vontade dos órgãos de gestão ou conselhos de administração.

2.1.3 Auditoria Interna

2.1.3.1 Conceito e Evolução

Em 1978 o IIA[4] definiu o conceito de auditoria interna como:

> […] "*an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes".*

A AI visa assegurar as políticas e procedimentos instituídos de forma a serem observados dentro da Organização. Tem como principal objetivo auxiliar a administração e apoiar a Organização contribuindo para a melhoria do desempenho da entidade empregadora.

Auxilia e acompanha a Organização na concretização dos seus objetivos, através de uma abordagem metódica e sistemática, de modo a avaliar e melhorar a efetividade dos métodos de controlo de riscos e gestão, atua de forma periódica visando também outras áreas, não só associadas à contabilidade, como por exemplo o sistema de controlo da qualidade ou a administração de pessoal.

Segundo Sawyer (2005, p. 837) numa empresa a AI compreende:

> «tudo o que o responsável pela função de Auditoria Interna quiser que esta seja, contando com o apoio da direção, com vista a uma melhor tomada de decisão por parte da gestão, no alcance dos objetivos e na prossecução de perspetivas para o futuro».

A AI é geralmente desempenhada por um colaborador da empresa nomeado pelo órgão de gestão para efetuar as verificações necessárias e avaliar os sistemas e procedimentos da empresa, com vista a minimizar as probabilidades de erros ou práticas ineficazes.

Poder-se-á considerar a AI como um controlo por parte do órgão de gestão que funciona por meio de medição e avaliação da eficiência e eficácia dos principais departamentos da Organização. É de salientar que no caso da AI as ações do auditor estão limitadas pelos requisitos definidos pelo órgão de gestão, no entanto os relatórios de AI destinam-se à administração da empresa e incidem sobre todas as funções económicas da empresa, estes relatórios devem ser independentes no seio da Organização.

[4] IIA - https://na.theiia.org/about-us/Pages/About-The-Institute-of-Internal-Auditors.aspx

Na opinião de Baharuddin, Lesetedi e Nieuwlands (2019) mediante o contributo e proatividade dos auditores é possível incrementar credibilidade e criar valor para uma Organização, bem como, as avaliações que estes fornecem permitem atingir novos conhecimentos e calcular impactos futuros, razão pela qual os profissionais de auditoria lideram cada vez mais em conjunto com os conselhos de administração e órgãos de gestão, estratégias capazes de transformar a perceção morosa na adoção de novos procedimentos internos e no alcance dos objetivos.

A AI deve ser compreendida, de modo sucinto, como uma atividade de auxílio à gestão relativo ao desempenho de cada departamento da empresa, mediante as diretrizes, políticas e objetivos que foram previamente determinados.

2.1.4 Sistema de Controlo Interno

Segundo Morais e Martins (2007) a primeira definição de controlo interno foi feita pelo *American Institute of Certified Public Accountants* (AICPA), em 1934, que estabelece controlo interno como "um plano de Organização e coordenação de todos os métodos e medidas adotadas num negócio a fim de garantir a salvaguarda de ativos, verificar a adequação e confiabilidade dos dados estatísticos, promover a eficiência operacional e encorajar a adesão às políticas estabelecidas pela gestão".

Os objetivos de auditoria passam por incluir para além das responsabilidades dos auditores e do relato na identificação de não conformidades a falta de eficácia do sistema de controlo interno. (Aguiar, 2014).

Segundo o *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) o controlo interno define-se como um processo, implementado pela direção de uma entidade, gestores e outro pessoal relevante, desenhado para proporcionar segurança razoável em relação ao alcance dos objetivos relacionados com as operações, reporte e conformidade com as leis e regulamentos (COSO, 2013). Segundo o COSO, observe-se a **Figura 2.1** onde são expostos os conceitos fundamentais sobre o controlo interno.

Figura 2.1 - Conceitos fundamentais de Controlo Interno

Fonte: Autoria Própria

Importa ainda dividir os controlos segundo o seu tipo e o seu objetivo. Sendo assim, é elaborada posteriormente a **Tabela 2.1** onde são relacionados os tipos de controlos.

Tabela 2.1 - Tipos de Controlos

Tipos de Controlos	**Objetivo**
Preventivos	Impedir a ocorrência de factos indesejáveis.
Detetores	Detetar factos indesejáveis já ocorridos.
Corretivos	Retificar problemas identificados.
Orientadores	Transmitir orientações para a ocorrência de factos desejáveis.
Compensatórios	Compensar fraquezas de controlo noutras áreas.

Fonte: Autoria Própria, adaptado de Morais e Martins (2007)

Complementarmente, cabe ao órgão de gestão implementar o Sistema de Controlo Interno (SCI) com vista à prevenção de presumíveis distorções materiais, bem como, a sua deteção caso estas ocorram. Tem ainda a responsabilidade de desenvolver, executar e manter um bom SCI, para assegurar a salvaguarda dos ativos e das transações.

Nenhum planeamento deverá realizar-se sem que sejam efetuados, uma análise prévia e um teste, aos sistemas instituídos. Como tal, para determinar a existência ou omissão de erros que alterem significativamente as demonstrações financeiras, o auditor estabelece e define a extensão dos procedimentos de auditoria e a sua execução. No entanto esses testes não são satisfatórios permitindo concluir se as demonstrações financeiras refletem corretamente os resultados das suas operações, não sendo possível ter uma segurança completa relativamente às demonstrações financeiras.

A avaliação do SCI serve de base para o auditor determinar o grau de confiança que nele possa depositar e a partir daí, fixar a natureza e extensão dos procedimentos de auditoria a serem adotados.

Resultante da identificação das fraquezas do controlo interno, o auditor pode efetuar recomendações pertinentes e mais realistas à administração para que providenciem as alterações que considerem apropriadas.

O SCI pode assim ser subdividido em três grupos segundo o Decreto Lei n.º 166/98, de 25 de junho[5]:

1- Operacional, que consiste na verificação, acompanhamento e informação, centrado sobre decisões dos órgãos de gestão das unidades de execução de ações é constituído pelos órgãos e serviços de inspeção, auditoria ou fiscalização inseridos no âmbito da respetiva unidade;

2- Setorial, que consiste na verificação, acompanhamento e informação perspetivados preferencialmente sobre a avaliação do controlo operacional e sobre a adequação da inserção de cada unidade operativa e respetivo sistema de gestão, nos planos globais de cada ministério ou região, sendo exercido pelos órgãos sectoriais e regionais de controlo interno;

[5] Art.º 4º, do Decreto-Lei n.º 166/98, de 25 de junho.

3- Estratégico, que consiste na verificação, acompanhamento e informação, perspetivados de preferência sobre a avaliação do controlo operacional e controlo sectorial, bem como, sobre a realização das metas traçadas nos instrumentos provisionais, designadamente o Programa do Governo, as Grandes Opções do Plano e o Orçamento do Estado.

2.1.5 *Control Objectives for Information and Related Technology* (COBIT) – A *Framework*

Segundo o referido pelo Mestre Osman Abdul Aziz, na sua dissertação denominada "Auditoria aos Sistemas de Informação com base *no Control Objectives for Information and related Techonology* (COBIT)" (2019, p.8), esta *framework*:

> «O COBIT 5 veio desempenhar um papel consolidador e fundamental na governação e gestão de TI, através de um modelo único e integrado devido ao seu alinhamento com outros padrões e modelos, tais como, ITIL, orientação a standards ISO, BSC, entre outros.
>
> O COBIT 5 junta os cinco princípios (...), que permitem a organização construir um modelo de gestão e de governação baseado em sete *enablers*, que otimizam o investimento em TI em benefício das partes interessadas (ISACA, 2012)».

Escrutinemos então esses mesmos cinco princípios referidos por Osman Aziz, segundo a sua investigação:

1. Atender às necessidades das Partes Interessadas.

Para Aziz (2019, p.9) «numa perspetiva de governação de TI, o principal objetivo do COBIT é permitir a criação de valor por meio da garantia de que os benefícios sejam percebidos, os riscos reduzidos e os recursos otimizados. Também é apresentado para fornecer às partes interessadas do negócio um modelo de governação de TI que aprimore a gestão dos riscos associados ao departamento de TI (Oliver, D., & Lainhart, J. 2012)».

2. Cobrir a organização numa visão ponta-a-ponta/abordagem à governação.

Segundo Aziz (2019, p.13) «o âmbito do COBIT 5 compreende toda a informação e tecnologia relacionada na Organização. Este princípio, inclui toda a gestão e governação abordada pelo departamento de TI, ou seja, por um lado, o sistema de governação TI, está inserido no sistema de governação de toda a organização, por outro lado, todas as funções e processos que são utilizados pela gestão e governação também estão incluídos.

Este é o significado a reter quando se fala numa Organização orientada a processos numa visão "ponta-a-ponta". De acordo com o COBIT 5, trata-se de uma "abordagem à governação"».

3. Aplicar um modelo único integrado

Refere ainda Aziz (2019, p.14) «o COBIT 5, apresenta um papel de modelo único e integrado devido a quatro razões principais:

3.1 - Considera as normas, padrões e *frameworks* mais recentes, permitindo que o COBIT 5 seja a estrutura principal que alinha todas as atividades de governação e gestão;

3.2 - Por integrar outras *frameworks*, normas e práticas, apresenta uma posição única e integrada em orientação com uma linguagem comum não técnica;

3.3 - É uma *framework* que resume e elabora guias de orientação, fornece um conjunto de elementos de apoio que incluem, ISACA Research, ITIL, TOGAF, ISO, bem como, uma série de instrumentos de apoio relacionados com o COBIT 5;

3.4 - Integra todo o tipo de informação presente nos diversos modelos da ISACA sobre governação e gestão de TI, assim como, as suas boas práticas».

4. Permitir uma abordagem holística

Complementa Aziz (2019, p.16) «para uma gestão e governação de TI ser eficiente e eficaz dentro de uma Organização, requer que seja considerado uma série de fatores díspares, designados de enablers[6].

Consequentemente quando são tomadas decisões, é necessário que exista o máximo de informação possível, ou seja, é necessária uma visão global e completa da Organização, nomeadamente, em termos de processos de gestão e de governação e toda a estrutura».

5. Distinguir a governação da gestão

Aziz (2019, p.17) menciona ainda que «o COBIT 5 faz uma clara distinção, indicando que cada um serve um propósito diferente com responsabilidades, atividades e estruturas organizacionais também diferentes.

[6] «Os enablers são aplicáveis ao nível de toda a Organização, incluindo todos os recursos, internos e externos, relacionados com o departamento de TI, bem como, as atividades e responsabilidades dentro e fora das funções de TI. Entende-se que cada enabler precisa de outro enabler para produzirem efeitos/resultados, por exemplo, processos precisam de dados e informação ou as estruturas organizacionais precisam de pessoas e competências» Aziz (2019, p.26).

O COBIT 5 utiliza as siglas, EDM e PBRM, respetivamente para governação e gestão. Sendo que EDM traduz-se para Avaliar, Orientar, Monitorizar (*Evaluate, Direct and Monitor*), e PBRM para Planear, Construir, Entregar e Monitorizar (*Plan, Build, Run and Monitor*).

A função de governação ou EDM, é a de garantir que as necessidades das partes interessadas são avaliadas de modo a determinar os objetivos organizacionais que têm de ser alcançados, define uma orientação através da escala 'P' e 'S' para melhor prioritização e tomadas de decisão e monitoriza o desempenho e a conformidade de acordo com os objetivos estabelecidos.

A função de gestão ou PBRM é a de garantir que as atividades estão alinhadas com as orientações indicadas pela função de governação».

2.2 Redes Móveis

A comunicação móvel e a evolução das redes móveis dura há praticamente 40 anos.

As redes de comunicações móveis atravessam tempos de mudança. Desde o ano de 2004 aquando do aparecimento da rede móvel 3G que se tem assistido a um crescente volume de tráfego na denominada rede móvel.

Foi a partir de 2004 que começou a verificar-se um aumento na diversidade de produtos e serviços oferecidos aos consumidores, mas foi a partir do ano de 2012 aquando do aparecimento do 4G que esta rede móvel começou a despertar interesse, muito por via dos *Smartphones*, os aparelhos indicados como os impulsionadores dos serviços de dados.

A partir desta realidade, a procura por este tipo de tecnologia e de melhores condições têm exigido um afincado empenho às operadoras para uma oferta de soluções, capazes de acompanhar tais evoluções, ao mesmo tempo que se tentam manter atrativas, inovadoras e competitivas.

Observe-se a seguinte figura (**Figura 2.2**), onde é elaborado um cronograma relativo ao 5G.

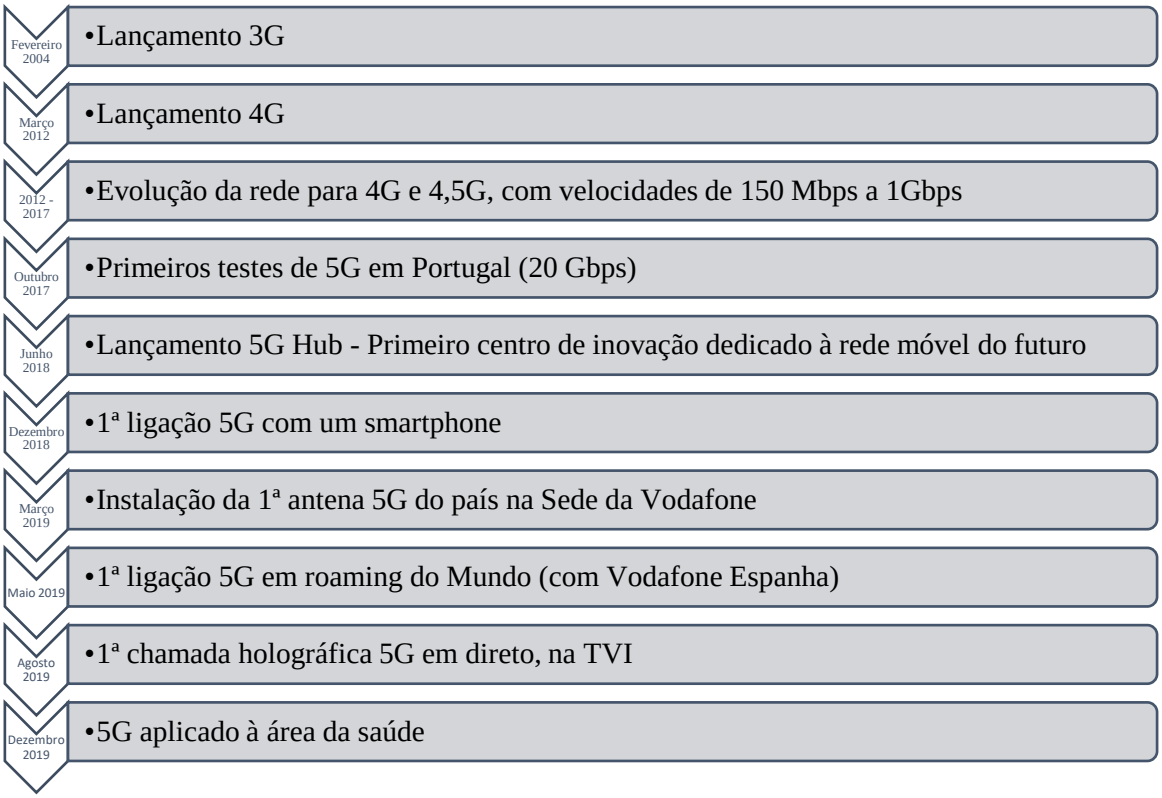

Figura 2.2 - Cronograma, Portugal a caminho do 5G

Fonte: Autoria Própria, adaptado da Vodafone

2.2.1 Evolução das Redes Móveis

A primeira geração de rede móvel (1G), como já referido na «Introdução», aparece em meados de 1980. Permitiu a transferência de dados de voz num sistema duplex, isto é, transmitir e receber comunicações em simultâneo numa comunicação *wireless* por meio de ondas analógicas.

Por serem a primeira geração, os aparelhos tecnológicos compatíveis com esta nova tecnologia não suportavam qualquer tipo de encriptação da informação e dos dados, o que originou inúmeros problemas de segurança.

O 1G ficou caracterizado na sua época pelas fracas limitações existentes relacionadas com o sinal analógico, pela fraca qualidade do som existente nas comunicações e pela baixa velocidade de transferência de dados que rondava os 9,6 Kilobytes (Kbps) o que provocava frequentes interrupções nas comunicações.

Passados mais de 10 anos (em meados de 1990), surge a rede móvel de segunda geração (2G) com o intuito de colmatar algumas limitações existentes no 1G, em particular, a melhoria da qualidade de transmissão e da cobertura do sinal. Com o 2G o analógico é posto de parte e dá lugar ao digital, nomeadamente ao *Global System for Mobile communications* (GSM).

Através do GSM foi possível criar diversos serviços, muitos deles ainda hoje usados, mormente o *Short Messaging Service* (SMS), o *General Packet Radio Service* (GPRS), o *Enhanced Data rates for GSM Evolution* (EDGE) ou o *High Speed Circuit-Switched Data* (HSCSD). Esta rede móvel ficou conhecida pela sua segurança, a sua robustez/fiabilidade, a sua utilização eficiente do espectro e pela sua transferência de dados até 500 Kbps. A tecnologia 2G ficou também caracterizada pelo mítico reinado e popularidade dos aparelhos da marca Nokia, entretanto adquirida pela Microsoft em 2013.

Passada mais uma década (ano 2000 e seguintes), emerge a rede móvel de terceira geração (3G) com o propósito de servir uma ampla gama de aplicações multimédia. O 3G ocasionou a criação do ainda hoje utilizado *Universal Mobile Telecommunications System* (UMTS), sistema esse que ainda hoje favorece a expansão e o aumento da qualidade dos serviços multimédia fornecidos pelas redes móveis.

Apenas com a chegada do 3G foi possível conectar os aparelhos tecnológicos à Internet para uma navegação na *web* com velocidades consideradas aceitáveis. O 3G proporcionou velocidades de 28 Megabytes (Mbps) e possibilitou o desenvolvimento de diversos serviços, muito utilizados nos dias correntes, sobretudo o *World Wide Web* (WWW), o correio eletrónico (*E-mail*) e o comércio eletrónico (*E-commerce*), razão pela qual a Microsoft tanto se interessou na aquisição da Nokia.

2.2.2 Rede Móvel 4G

A rede 4G tal como a própria sigla indica, refere-se à quarta geração de rede móvel. Este tipo de rede é vulgarmente associado a uma outra sigla, mas que muito diz sobre ela, a 4G LTE. A tecnologia LTE vem do inglês *Long Term Evolution* e é a principal característica desta rede móvel.

O seu aparecimento veio sobretudo agilizar a velocidade de tráfego das redes móveis chegando a permitir mesmo uma velocidade máxima de 100 Mb por cada segundo. Com a implementação da rede móvel de quarta geração associada à tecnologia LTE foi possível também o desenvolvimento da atual televisão digital terrestre, a conhecida TDT.

Apesar de ainda existirem dispositivos atualmente compatíveis com esta tecnologia, convém referir que o 4G apareceu em Portugal por volta de 2009. Desde então já muitas são as suas mutações e avanços, ao ponto de em meados de 2014 ter sido lançada "digitalmente" a rede 4G + ou 4G *plus*. Estas redes triplicaram as velocidades e os desempenhos obtidos pela anterior rede de quarta geração.

2.2.3 Rede Móvel 5G

A rede 5G pode ser caracterizada como a sucessão natural da rede móvel de quarta geração, que trará mais do que uma conexão entre pessoas a velocidades extremas e com ínfimas latências temporais. Trará a possibilidade de as pessoas poderem controlar diversos dispositivos e/ou variados aparelhos utilizados no seu dia-a-dia.

A fácil e rápida implementação desta nova rede será permitida através da já utilizada tecnologia LTE, tecnologia essa utilizada para a distribuição do sinal de rede móvel.

Em suma, o objetivo desta nova rede de quinta geração passa por trazer soluções para determinadas situações com associação à IoT e assim tornar exequível que as pessoas que usufruem e consomem este tipo de tecnologia, tenham experiências diferenciadas através de uma rede mais rápida.

Complementarmente, a capacidade de transmissão de dados é muito maior e integra um reduzido consumo de energia em comparação com a rede atualmente em vigor.

Existe a previsão de que num futuro próximo, a rede de quinta geração possibilite às pessoas uma utilização mais consciente e eficiente da mesma, bem como, um controlo mais otimizado dos consumos energéticos, tornando assim a rede 5G uma rede muito ambicionada e que se espera seja de implementação total a curto prazo.

2.2.4 A Novidade 5G

Após uma análise às redes, particularmente entre o 5G e as anteriores (4G por exemplo), é impossível que não sobressaia, tecnicamente, uma enorme diferença esperada na latência nesta nova rede. Atualmente a latência na rede de quarta geração situa-se entre 80 e 100 milésimos de segundos.

Prevê-se que a latência na rede de quinta geração passe para cerca de 10 milissegundos. Se o tempo de latência é já atualmente em certas circunstâncias muito reduzido, podemos imaginar a instantaneidade esperada no 5G.

Tal latência irá permitir entre outras coisas a tão desejada condução de veículos automóveis de forma autónoma. Já existem protótipos de viaturas sem condutor que procuram dar resposta a necessidades concretas.

Com todas as novas novidades esperadas com a rede de quinta geração, os atuais nove biliões de aparelhos conectados à rede móvel 4G irão crescer para cerca de vinte biliões durante o decorrer dos próximos anos, apenas com a implementação desta nova geração.

Neste pressuposto, observe-se a seguinte figura (**Figura 2.3**), onde são esquematizadas as principais vantagens do 5G.

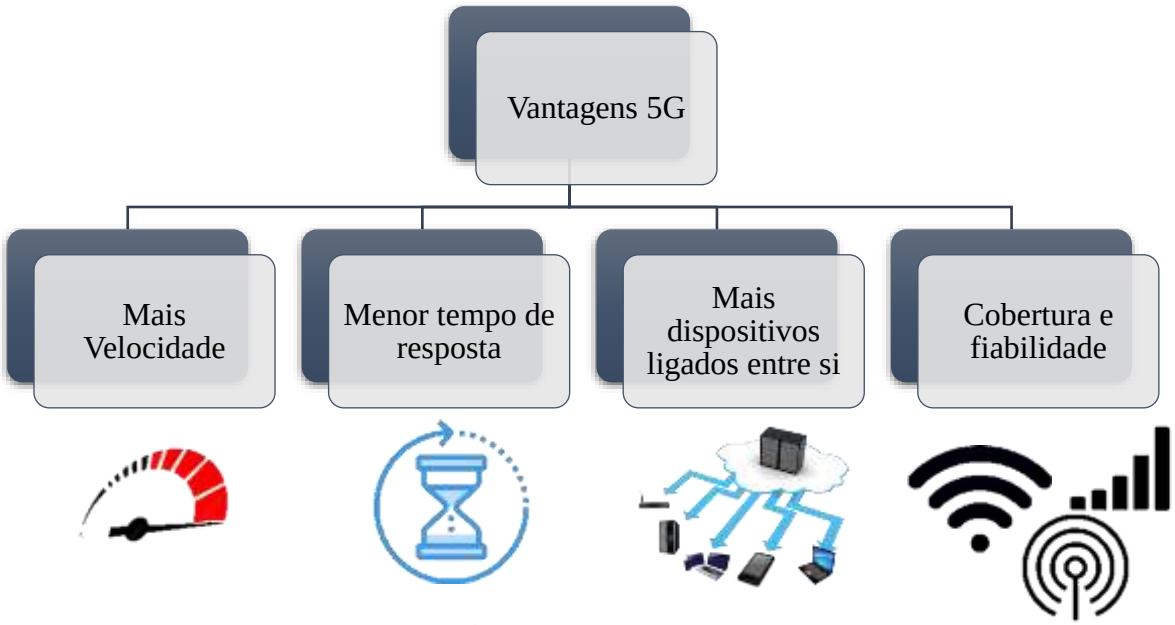

Figura 2.3 - Vantagens 5G

Fonte: Autoria Própria, adaptado da Vodafone

Resultante da identificação das novidades provenientes da implementação do 5G, podemos identificar três novidades fundamentais. São elas as seguintes:

1- Uma velocidade de navegação dez vezes superior à utilizada atualmente;

2- Uma menor latência, isto é, o tempo resultante da conexão entre dois pontos de rede (o terminal como um telemóvel e o seu servidor);

3- Uma maior conexão por quilómetro quadrado de novos aparelhos os denominados sensores e terminais de IoT.

2.2.5 Análise SWOT ao 5G

Kenneth Andrews e Roland Christensen, ambos professores de Harvard, ao terem proposto ao mercado uma avaliação diagnóstica conhecida por Análise SWOT, em que clarifica a posição competitiva de uma empresa no mercado, o objetivo é caracterizar os pontos fortes e fracos, as ameaças e as oportunidades perante os desafios existentes.

Entende-se, pois, através do recurso a uma matriz de eixos a importância de diagnosticar o ambiente 5G, em que os pontos fortes e pontos fracos são internos à Organização, as oportunidades e as ameaças relativas ao meio envolvente, mas que são externas à Organização.

Ao relacionarem-se estas duas dimensões que se complementam entre si, designadamente a importância de uma análise externa e uma interna, o momento será crítico no qual os decisores utilizam os pontos fortes e procurarão obter vantagens no aproveitamento das oportunidades.

No sentido oposto, evitar as ameaças faz parte do desenvolvimento de uma estratégia clara para mitigar os pontos fracos, potenciando o que realmente interessa (Forças e Oportunidades). Deste modo, procura-se neutralizar sempre que possível as fragilidades (Fraquezas e Ameaças) numa orientação clara sobre a gestão do risco relacionado com o negócio.

Cada Organização terá que listar os diversos elementos que a envolvem, associar a sua cultura organizacional, extrair as vantagens de adaptar novas tecnologias perante cenários de crise, procurar realizar benchmarking com a concorrência e em contrapartida, analisar os efeitos dos seus pontos fracos que devem ser discutidos e trabalhados.

Uma aposta clara nas vantagens competitivas existentes irá permitir evidenciar os pontos fortes, investindo na neutralização dos pontos fracos. Ambos são possíveis de controlar e monitorizar. Perante as vantagens do 5G, é essencial compreender as reais ameaças que não se controlam e até podem nunca vir a existir.

Quanto a oportunidades, o futuro é sempre uma incógnita, ainda para mais em fases pandémicas em que a COVID-19 tem dominado as atenções.

Neste contexto, observe-se a figura (**Figura 2.4**), onde é esquematizada uma análise de Forças (*Strengths*), Fraquezas (*Weaknesses*), Oportunidades (*Opportunities*) e Ameaças (*Threats*) do 5G.

PONTOS FORTES	PONTOS FRACOS
• Internet móvel muito mais rápida; • Baixa latência; • Maior cobertura; • Mais programável.	• Demora na implementação; • Muitos dos atuais dispositivos ficarão obsoletos; • Implementação com custos elevados.

OPORTUNIDADES	AMEAÇAS
• Impulsionar tecnologias imersivas; • Propensão dos consumidores por novos produtos; • Apresentam produtos com preços competitivos; • Realidade Aumentada (AR) e Realidade Virtual (VR); • Condução autónoma e medicina remota.	• IoT do 5G poderá criar problemas de segurança; • Entrada de novas empresas para o mercado; • Comparabilidade de preços com o espaço europeu; • Comunicação segura, gestão identidade, privacidade e garantia de segurança; • Cibersegurança.

Figura 2.4 - Análise SWOT 5G

Fonte: Autoria Própria

2.2.6 Impactos das Redes Móveis nas Empresas

A pandemia que atravessamos aumentou a dependência das redes móveis e por consequência os eventos cibernéticos ganham maior destaque pela severidade que podem significar nas operações das Organizações. Estas que até há pouco tempo tinham parte da sua atividade assente em processos manuais, tornaram-se dependentes das redes móveis e de aparelhos tecnológicos para poderem concretizar de forma mais rápida os seus negócios.

As rotinas diárias para as empresas mudaram e o novo paradigma "potenciou a exposição a riscos e vulnerabilidade no que à segurança cibernética diz respeito", sustenta Pedro Pinhal da MDS *Brokerslink* Portugal.

Assim sendo, a COVID-19[7] tem criado condições para o aumento exponencial dos riscos cibernéticos por via da necessidade de informação e dos receios quanto à pandemia, que estão a ser usados por grupos maliciosos que aproveitaram este novo contexto para lançar vários ataques, por exemplo, através de *Malicious Domains, Online Scams* e *Phishing, Malware, Ransonware* e *DDoS*.

[7] A Organização Mundial da Saúde (OMS) atribuiu o nome, COVID-19, cujo nome da doença resulta das palavras "**Co**rona", "**Ví**rus" e "**D**oença" com indicação do ano em que surgiu (20**19**). SARS-CoV-2 é o nome do novo coronavírus que foi detetado na China, no final de 2019 e que significa "síndrome respiratória aguda grave – coronavírus 2". A COVID-19 é a doença que é provocada pela infeção pelo coronavírus SARS-CoV-2.

Importa também clarificar o que se entende por *Phishing*[8], *Malware*[9], *Ransonware*[10] e *DDoS*[11]. Com particular evidência, os ataques cibernéticos como por exemplo, o roubo de informações, a divulgação de dados de clientes, fornecedores e colaboradores e até a interrupção das atividades, já faziam parte da realidade empresarial e das sociedades.

Todavia, em consequência de um acesso cada vez mais massivo à Internet, através do aumento do número de utilizadores, com a necessidade de guardarem e partilharem informações em rede, a segurança no ciberespaço deve e tem de passar a ser encarada pelas Organizações e pelos utilizadores de maneira diferente. A auditoria tem um papel relevante.

Com a evolução das redes móveis as sofisticações dos ataques também evoluíram. Por exemplo, ao nível do teletrabalho que está a ser imposto pela pandemia COVID-19, as orientações laborais associadas ao aumento das atividades e tarefas, fez disparar os ataques de *Phishing* com novos métodos que aproveitam o trabalho hoje efetuado remotamente.

2.3 Cibersegurança

De acordo com a Resolução do Conselho de Ministros n.º 92/2019 de 5 junho, foi aprovada a Estratégia Nacional de Segurança do Ciberespaço 2019-2023, que determina a elaboração de um Plano de Ação da Estratégia Nacional de Segurança do Ciberespaço, competindo ao Centro Nacional de Cibersegurança, enquanto Autoridade Nacional de Cibersegurança, a coordenação da elaboração, o acompanhamento da execução e a revisão do Plano de Ação referido, em articulação e estreita cooperação com todas as entidades com responsabilidade no âmbito da segurança do Ciberespaço.

[8] Segundo o Relatório de cenário de ameaças da Agência da União Europeia para a Cibersegurança (ENISA) de 28 de janeiro de 2019, o *Phishing* consiste no mecanismo de elaboração de mensagens que usam técnicas de engenharia social de modo a que o alvo seja ludibriado 'mordendo o isco'. Mais especificamente, os atacantes tentam enganar os recetores de *emails* ou mensagens para que estes abram anexos maliciosos, cliquem em URL inseguros, revelem as suas credenciais através de páginas de *Phishing* aparentemente legítimas (*Pharming*), façam transferências de dinheiro, entre outras.

[9] Segundo o Glossário dos principais termos de segurança de informações do Instituto Nacional de Padrões e Tecnologia, o *Malware* consiste no programa que é introduzido num sistema, geralmente de forma encoberta, com a intenção de comprometer a confidencialidade, a integridade ou a disponibilidade dos dados da vítima, de aplicações ou do sistema operativo, ou perturbando a vítima.

[10] Segundo o Relatório de cenário de ameaças da Agência da União Europeia para a Cibersegurança (ENISA) de 28 de janeiro de 2019, o *Ransomware* consiste no tipo de *software* malicioso que permite que "um atacante se apodere dos ficheiros e/ou dispositivos de uma vítima, bloqueando a possibilidade de esta poder aceder-lhes. Para a recuperação dos ficheiros, é exigido ao proprietário um resgate em criptomoedas".

[11] Significa *Denial of Service* e de forma muito resumida é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores.

Esta estratégia procura afirmar-se como necessária na explanação de alguns dos conceitos mais relevantes neste âmbito, permitindo a constituição de uma base de entendimento geral que possa ser compreendida por todos. Importa clarificar o termo Cibersegurança, entre outros, que este diploma legal consagra:

> «[C]ibersegurança consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço e das pessoas que nele interagem.»

2.3.1 Riscos Cibernéticos

Com um mundo cada vez mais digital é impreterível que apareçam riscos com a atualização massiva da Internet e dos seus derivados. São os denominados riscos cibernéticos.

Atualmente existem diversos tipos de riscos cibernéticos e com a avançar do tempo e da tecnologia é natural que apareçam muitos outros.

Complementando as definições já apresentadas podem ainda ser tipificados os seguintes riscos cibernéticos:

- O *Malware*, basicamente, é um software malicioso. Está normalmente associado a um programa ou ficheiro que contém na sua composição *worm's*, *spywares* e os mais comuns vírus que se instalam num qualquer computador;
- O *Ransomware*, cuja principal característica é bloquear programas e/ou ficheiros do lesado, criptografando os mesmos e coagindo o utilizador que necessita ter acesso (e deixa de ter) a um pagamento para reaver os seus programas e/ou ficheiros;
- O *Phishing*, que significa por exemplo, um correio eletrónico fraudulento que se faz passar por fontes respeitáveis, com a única intenção de lesar por meio de roubo dados confidenciais. Os mais comuns são os dados do cartão de crédito e informações de autenticação *login* e palavra passe.

Para que seja garantida uma correta e eficaz segurança cibernética é necessário que exista por parte dos SI, uma forte segurança em aplicativos em informações e também na rede, mas sobretudo uma educação e consciencialização por parte do utilizador.

2.3.2 Diretiva NIS

A diretiva NIS foi implementada no dia 6 de julho de 2016 e está diretamente associada à segurança das redes e da informação.

NIS provém do inglês *Network and Information Security* e retrata a primeira legislação proferida no Espaço *Schengen* sobre e para a Cibersegurança, que decreta diversas medidas com vista à prevenção de incidentes cibernéticos em território europeu.

Entre essas medidas estão presentes a plena cooperação entre si de todos os países do espaço *Schengen* relativamente à matéria dos crimes cibernéticos, bem como, a intenção de criar uma cultura de segurança nomeadamente em setores sensíveis para a economia e para a sociedade que estão dependentes maioritariamente das Tecnologias de Informação (TI).

É possível observar através da leitura da diretiva que a mesma decreta a formação de equipas especializadas e focadas em dar resposta aos possíveis acontecimentos cibernéticos, uma em cada país do Espaço *Schengen*, as equipas especializadas *Computer Security Incident Response Team* (CSIRT).

2.3.3 Lei Sobre Segurança Cibernética

Com o intento de acompanhar a atualidade foi criada no dia 13 de agosto de 2018, a Lei n.º 46/2018 que formula em Portugal o regime jurídico de segurança no ciberespaço através de medidas com o objetivo claro de assegurar um digno nível de segurança tanto nas redes como nos SI.

Trata-se de uma lei amplamente abrangente aplicando-se a inúmeras áreas desde a Administração Pública até qualquer entidade que faça uso de redes e qualquer tipo de SI.

A lei sobre a segurança cibernética foi criada como complemento até às então leis já existentes, nomeadamente, a lei sobre a proteção de dados pessoais para que fosse dada uma resposta mais rápida e eficaz aos incidentes de segurança informática a nível nacional.

2.3.4 Gabinete Nacional de Segurança e Centro Nacional Cibersegurança

O Centro Nacional de Cibersegurança (CNCS) reúne um conjunto de competências e integra o departamento do Gabinete Nacional de Segurança (GNS). Como o próprio nome indica, associa tudo o que se relaciona com o ciberespaço e consequentemente a cibersegurança a nível nacional. É a autoridade portuguesa competente e certificada que tem como objetivo garantir que os utilizadores registados dentro do território nacional utilizem o ciberespaço de uma maneira consciente, sem limitações, mas sobretudo de uma maneira segura.

O CNCS tenta dar aos utilizadores nacionais uma melhoria constante da qualidade da sua Cibersegurança através de uma crescente cooperação entre todas as autoridades competentes pela Cibersegurança a nível global.

Para além de toda a cooperação internacional, o CNCS coopera regularmente com diversos organismos nacionais afetos tanto à ciberespionagem, passando pelo cibercrime e pelo ciberterrorismo.

Tal cooperação tem permitido um constante aperfeiçoamento na utilização do ciberespaço por via da antecipação de situações que colocariam em risco o ciberespaço nacional.

A CNCS tem por isso os objetivos bem delineados que podem ser sumarizados numa atempada deteção, numa rápida reação e numa clara obstrução à ocorrência de incidentes cibernéticos. Tais objetivos delineiam claramente as competências do CNCS que passam por regular, regulamentar, supervisionar, fiscalizar, incluindo até o poder sancionatório para todos os assuntos relacionados com o ciberespaço e a Cibersegurança.

O tema da proteção de dados tem estado em constante escrutínio. É o CNCS a instituição responsável em articulação com a Comissão Nacional de Proteção de Dados (CNPD) pelo acompanhamento, monitorização e registo dos incidentes ocorridos relacionados com os dados pessoais.

2.4 Regulamento Geral da Proteção de Dados

Sendo as informações e os dados um dos "bens" mais preciosos para as organizações, tanto os seus como os dos seus clientes, é de todo relevante que estes sejam recolhidos e armazenados de forma correta e segura. Assim sendo e estando cada vez mais esta temática relacionada com a cibersegurança, a regulamentação para a proteção destes torna-se um tema impossível de contornar.

Em 2018 foi criado o RGPD com o propósito de se regular a proteção de dados pessoais aquando da sua recolha e do seu tratamento. Importa definir dados pessoais como sendo os dados que possibilitam a identificação do seu titular ou que a este estejam afetos, seja a nível imagem e voz, como a um nível biométrico ou escrito.

O RGPD veio revogar a diretiva até então existente “Diretiva de Proteção de Dados Pessoais de 1995 (95/46/CE)”. Passou a conter cláusulas e procedimentos obrigatórios da forma como são recolhidas e mais tarde tratadas as informações pessoais dos cidadãos residentes na União Europeia. Com a implementação deste regulamento os processos para a recolha destes dados passam a ter de ser modelados e analisados desde o seu início através de um padrão.

Um padrão com determinadas especificações e que cumpram certas obrigações, isto é, aquando da recolha dos dados, os mesmos devem ser armazenados de uma forma totalmente anónima e devem estar seguros através de elevados princípios, padrões e mecanismos de privacidade de modo que estes não estejam ao alcance de terceiros sem o respetivo consentimento dos visados.

O RGPD impõe limites e proibições para tratamento e uso de quaisquer tipos de dados pessoais fora do âmbito legal. Dá ao seu titular legítimo a possibilidade de a qualquer momento, solicitar o cancelamento ou anulação do seu consentimento para a recolha dos seus dados pessoais.

2.4.1 ePrivacy

Perante o exponencial aumento de tráfego de dados que existe por causa das redes móveis e sendo o ciberespaço uma crescente preocupação, muito em virtude da quantidade de dados que se tornam vulneráveis aquando da sua partilha através da internet, é de todo relevante abordar- se a regulamentação relacionada com este tipo de tecnologia.

O ePrivacy (ePR) é o regulamento europeu que aborda diversos tópicos, nomeadamente, os afetos à privacidade através da utilização das redes móveis e eletrónicas.

Em termos legais e não leigos o ePR é "Regulamento do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção de dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58 / CE (Regulamento de Privacidade e Comunicações Eletrónicas) ".

Em complemento ao RGPD, o ePR sugere matérias muito bem delineadas, designadamente, a confidencialidade nas comunicações e/ou o controlo da privacidade aquando do consentimento através de todos os meios eletrónicos ligados a uma qualquer rede móvel.

Conforme o constante na página online da Comissão Europeia, a proposta apresentada para o Regulamento do ePR ainda está por finalizar, mas já é possível ter uma perceção de algumas matérias delineadas, segundo as linhas condutoras sobre a privacidade, mas sobretudo da obrigatoriedade da sua aplicabilidade não só para as maiores empresas que atuam em território português, conhecidas pela distribuição de serviços de redes móveis e eletrónicas e que são operadores de telecomunicações (NOS, MEO, Vodafone) mas também para as empresas mundialmente conhecidas pela utilização das suas plataformas através de dados móveis (WhatsApp, Facebook Messenger, Skype, Instagram, entre outras).

Com esta vasta abrangência de entidades a Comissão Europeia pretende garantir a mesma exigência de grau de privacidade no uso de comunicações através de redes móveis e eletrónicas tanto para os operadores de telecomunicações como para as empresas detentoras das plataformas anteriormente mencionadas.

2.5 Sistemas de Informação

O termo SI é definido por Buckingham (1987) como sendo um sistema que congrega, guarda, processa e disponibiliza diversas informações de extrema relevância seja para uma determinada entidade ou para qualquer sociedade, de forma que tais informações estejam e sejam tanto acessíveis como uteis para todos aqueles que desejem usá-las.

Buckingham conclui que um SI é um sistema de atividade humana (social) que pode ou não envolver o uso de sistemas computadorizados.

Poder-se-á ter também em consideração uma frase proferida por Alter em 1992 que definiu SI como sendo: “uma congregação de informação, pessoas e TI, estruturadas por forma a alcançar determinados objetivos dentro das entidades”.

Com base nestas definições intemporais é possível identificar quatro tipos de SI apresentados na **Tabela 2.2** como se pode observar em seguida.

Tabela 2.2 - Tipos SI

Tipos de SI	Definição
***Enterprise Resource Planning* (ERP)**	Denominados *Enterprise Resource Planning* ou em português planeamento de recursos da empresa são softwares/programas que agregam diversos processos e dados de uma determinada entidade, no mesmo sítio. Dessa forma todos os processos e dados provenientes de diversas/os áreas/departamentos ficam localizados todos no mesmo local e acessíveis à maioria das pessoas autorizadas.
***Customer Relationship Management* (CRM)**	Intitulados *Customer Relationship Management* ou em português, gestão do relacionamento com os clientes que consistem em softwares/programas que incluem todos os mecanismos associados ao contato com os clientes. Neste sentido permite que as entidades. por exemplo, recolham e armazenem dados, assim como os gostos ou preferências, o histórico de pesquisas e compras de cada cliente, entre outras funcionalidades.
***Supply Chain Management* (SCM)**	Designados *Supply Chain Management* ou em português, gestão da cadeia de distribuição estão afetos a diversos procedimentos relativos à criação de valor para o consumidor final. São softwares/programas que compilam diversos dados desde os fabricantes/fornecedores até aos pontos de venda ao consumidor para que este encontre sempre em *stock* aquilo que procura. Assim é possível fazer uma previsão de vendas futuras, ter um controlo do inventário e reduzir custos em excesso.
***Management Information System* (MIS)**	Chamados *Management Information System* ou em português, sistema de informação de gestão são programas ou conjunto de programas que se complementam entre si e que ajudam as entidades nos seus processos laborais diários. Podem atuar tanto a nível estratégico como operacional e dão origem aos comuns relatórios apresentados e analisados nas tomadas de decisão.

Fonte: Autoria Própria, adaptado de Andrade e Julião (2019)

Capítulo III – Enquadramento Teórico

3.1 Enquadramento ao Estudo Empírico

No âmbito da presente dissertação e em alinhamento ao Estudo Empírico, destacam-se a veracidade dos temas de investigação, que são os seguintes:

T1: A nova fronteira de proteção de dados associados à Cibersegurança.

T2: Evidências ou falta delas de que o 5G é um real perigo para a Cibersegurança.

T3: Controlo da ASI relativamente a eventuais danos colaterais.

Estes temas devem-se ao facto de se considerarem ser os mais relevantes para o Estudo Empírico da ASI ao 5G no âmbito da Cibersegurança.

As evidências existentes e decorrentes da nova fronteira da Cibersegurança, referida por *Operational Technology* (OT)/ Tecnologia Operacional (TO) poderá vir a tornar-se um caso real preocupante não só em Portugal, como em todo o mundo. Este tipo de tecnologia está diretamente associado à monitorização e ao controlo de um grande leque variado e diversificado de elementos físicos.

Neste alinhamento, é impreterível a análise do 5G relativamente a um tema de destaque atual, a Cibersegurança, uma vez que esta nova tecnologia promete ser totalmente inovadora. Está atualmente em curso a sua implementação em Portugal e é um projeto que ainda não está totalmente instalado. Todavia e garantidamente, as suas implicações tecnológicas estão diretamente relacionadas com a Cibersegurança.

Por sua vez, a ASI é cada vez mais importante para que se consigam evitar danos colaterais a médio longo prazo, nomeadamente, no que diz respeito às normas de segurança e de proteção de dados dos utilizadores.

3.2 Metodologia e Procedimentos

Em concordância com Baptista e Sousa (2011),

> «[…] a metodologia de investigação consiste num processo de seleção da estratégia de investigação, que condiciona, por si só, a escolha das técnicas de recolha de dados, que devem ser adequadas aos objetivos que se pretendem atingir».

Para uma detalhada análise ao Estudo Empírico foram realizados vários trabalhos de pesquisa em diversas áreas e trabalho de campo, em concreto, a de maior recolha de informação foi realizada durante a feira mundial de tecnologia, *Web Summit* (WSS), totalmente relacionada com os temas acima referidos.

A escolha dos temas baseou-se no facto de, em comparação com outros que podiam ter sido considerados, serem de todo relevantes na sua análise e discussão de resultados, dada a ênfase das apresentações vivenciadas, comunicações tornadas públicas e outras abordagens que tenham influência no futuro da auditoria.

3.2.1 Conversas Informais

Foram realizadas conversas informais na WSS, a maior conferência de tecnologia, inovação e empreendedorismo de toda a Europa e que ocorre anualmente. Nos últimos anos é em território nacional, mais precisamente na Feira Internacional de Lisboa (FIL) que o evento decorre com enorme adesão presencial no anfiteatro do MEO Arena no Parque das Nações. Em 2020 por consequência das regras sanitárias impostas pela DGS, pela Organização Mundial da Saúde (OMS) e relacionadas com a COVID-19, o evento foi realizado online, tendo tido igualmente uma boa adesão.

É um evento muito emblemático e impactante. Em 2019 e durante os quatro dias em que o evento se realizou, foi anunciada uma mobilização de cerca de 50 000 pessoas de todo o mundo, situação que evidencia a importância de Lisboa como palco de participação.

Em termos de mediatismo do evento, foram mobilizados cerca de 2 000 jornalistas, investidores, diversos empreendedores, distintos políticos, notáveis empresários, mas sobretudo, estavam representadas cerca de 15 000 entidades em stands de menor destaque. Destas, cerca de 7 000 empresas procuraram destacar-se com stands diferenciados, entre elas empresas de auditoria, como a KPMG e também as denominadas pela WSS como as "entidades mais promissoras".

Durante os quatro dias de evento, assistimos a conferências de diversos temas relacionados com música, indústria automóvel, tecnologia financeira, saúde na era digital, marketing, robótica, desporto, entre outras, dos mais variados que possam existir tendo todos eles um elo em comum, a tecnologia.

Foi na WSS também que se possibilitaram diversas conversas informais cujo propósito é o reforço do objetivo da dissertação, sendo uma das técnicas de recolha de informações utilizadas na investigação em termos qualitativos, que segundo (Ketele,1999) citado por (Baptista & Sousa, 2011, p. 79) "consiste em conversas orais, individuais, ou de grupos, com várias pessoas cuidadosamente selecionadas, cujo grau de pertinência, validade e fiabilidade é analisado na perspetiva dos objetivos da recolha de informações".

Entre as conversas informais efetuadas, foi realizada uma com um colaborador da empresa Nokia em Portugal, que preferiu manter-se anónimo, mas que permitiu que o resultado da conversa fosse suscetível de publicação nesta dissertação. O interveniente exercia, há data da conversa, funções ligadas à área de engenharia de software (*Software Engineer*) e da conversa realizada, foi possível perceber que o mesmo entende que ainda existem muitas informações sobre o 5G e sobre outro tipo de informações/assuntos que daí possam surgir que necessitam de resposta e de um profundo estudo.

Apesar disso no decorrer da conversa, foi percetível aferir pelas afirmações do interveniente que a *Nokia Corporation* (empresa mãe) já anda a fazer diversos testes com esta nova tecnologia e a obter bons resultados com esses mesmos testes. Com o sucesso alcançado na testagem do 5G a Nokia está a fechar alguns negócios com operadoras de todo o mundo, no entanto apesar de tamanho sucesso terá de efetuar um corte em diversas despesas operacionais para que se consiga focar, pesquisar e investir nesta nova tecnologia, tentando voltar ao mercado com uma posição favorável como aconteceu à alguns anos atrás com o aparecimento dos telemóveis. Em resumo, foram apontados três pontos fundamentais:

- Automatização de sistemas;
- Processos simplificados;
- Redefinição de prioridades e investimentos no seu negócio que são as redes móveis.

Todavia, ao contrário do que se possa pensar e do que era esperado pela grande maioria dos participantes do evento, o tema do 5G não foi dos temas principais, sendo apenas falado e referenciado em algumas das conferências e nessas, retratado muito esporadicamente.

Em consonância com o ambiente vivido na WSS, William Blake Poeta afirma que «*[W]hat is now proved was once only imagined.*»[12] e como tal alguns oradores afirmaram que o 5G irá fazer muito mais do que simplesmente fazer um *upgrade* aos dispositivos que hoje nos rodeiam e que nos podem facilitar em todos os momentos no nosso dia-a-dia, como por exemplo, conseguir ver o interior do nosso frigorifico e saber o que precisamos de comprar, abrir e fechar persianas, acender e desligar luzes, ligar o sistema de rega, etc.

Toda esta revolução, inovação e *upgrade* no mundo tecnológico e na capacidade de comunicação de dados entre dispositivos irá potenciar o aparecimento e evolução de serviços e de aplicações dificilmente hoje imagináveis. No entanto e como em tudo o que acontece em termos globais e no mundo tecnológico em particular, a implementação do 5G terá de ultrapassar certos e determinados desafios que podem ir desde a construção e elaboração de infraestruturas de apoio e suporte até aos ataques cibernéticos e fraquezas que possam ser deixadas a descoberto com esta nova tecnologia.

3.3 Exposição dos Temas de Investigação

T1: A nova fronteira de proteção de dados associados à Cibersegurança

Este primeiro tema procura clarificar a veracidade da investigação. Se não houver a ocorrência de mais nenhum imprevisto ou nova pandemia que afete o mundo, os especialistas afirmam que, nos próximos dois/três anos, a próxima geração de rede móvel (o 5G) será uma certeza e algo, um tanto ou quanto banal nas nossas vidas, apesar do grande salto que se irá dar com a implementação desta nova tecnologia.

O 5G proporcionará um mundo "todo ligado entre si", caracterizado por transferências de dados extraordinariamente rápidos, alta conetividade e um volume de tráfego de dados na casa dos triliões de bytes.

Tal conexão permitirá uma monitorização direta ou sob controlo, de diversos dispositivos através do seu *hardware* e/ou *software*, a denominada Tecnologia Operacional (TO).

[12] «[O] que é agora comprovado foi um dia imaginado»

Apesar da tão esperada TO, o 5G também possibilitará o aparecimento e evolução de diversos tipos de tecnologias disruptivas que criaram novos desafios, nomeadamente, em relação à proteção de dados e assim trazer novamente para a ribalta as preocupações com a Cibersegurança.

Resume-se assim que, com a implementação da quinta geração de rede móvel, da evolução da TO e do aparecimento de novas tecnologias disruptivas irão aumentar as preocupações ao nível da Cibersegurança.

Se atualmente já existem algumas preocupações significativas de Cibersegurança ao nível do roubo de dados e apenas se discutem gigabytes (biliões de bytes) de tráfego de dados, imagine-se quando for implementado o 5G que se iram discutir Zettabytes (triliões de bytes) de tráfego de dados. Para que se entenda a complexidade do tráfego de dados observe-se o seguinte índice de bytes na **Figura 3.1.**

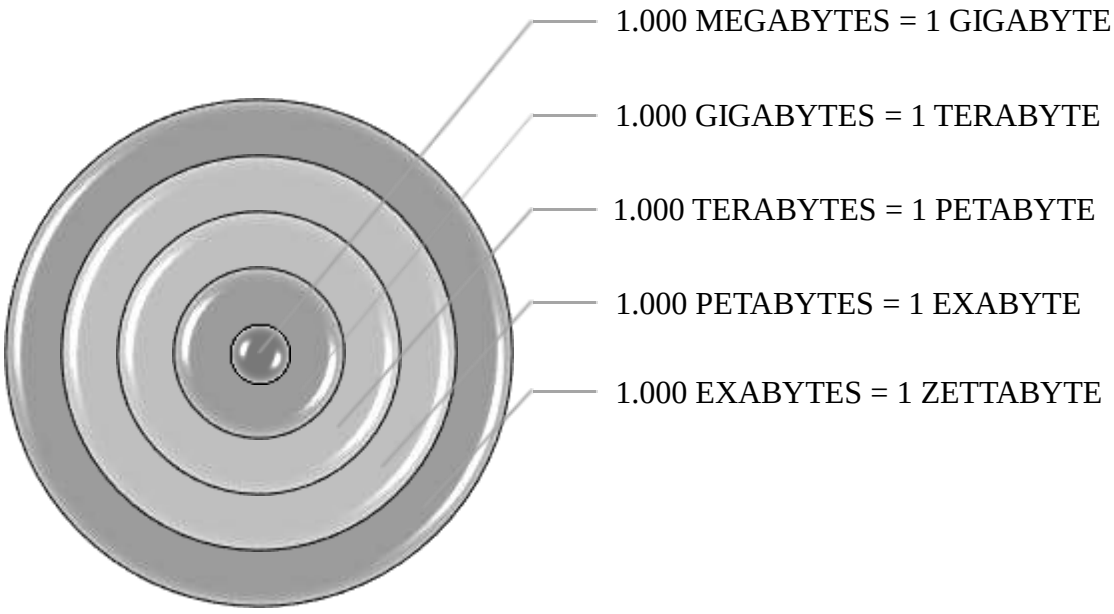

Figura 3.1 - Índice bytes

Fonte: Autoria Própria

Com a análise da figura é possível aferir que o tráfego de um Zettabyte de dados irá corresponder a muitos dados em trânsito ao mesmo tempo e por isso será cada vez mais imprescindível uma boa e correta análise dos dados.

Sendo assim, será necessário que existam pessoas qualificadas para a análise de todos estes dados e que os possam decompor/dividir em grupos de dados para que posteriormente se possa retirar informações e entendimentos sobre tais grupos de dados. Para além de pessoal qualificado na área de análise de dados, também os auditores terão de se qualificar, para que também eles possam estar na posse de ferramentas de análise de populações totais de dados e possíveis correlações, aperfeiçoando assim, as suas aptidões de avaliação, a oportunidade de aferir novos conhecimentos e a possibilidade de delinearem previsões.

Para justificar esta pertinência e segundo as normas internacionais para a prática profissional de AI no *The Institute of Internal Auditors* (The IIA) é possível verificar na norma 1220 intitulada "Zelo Profissional Devido":

> «1220 – Zelo Profissional Devido
>
> Os auditores internos devem empregar o zelo e habilidades esperados de um auditor interno razoavelmente prudente e competente. O zelo profissional devido não implica em infalibilidade.
>
> 1220.A1 – Os auditores internos devem exercer o zelo profissional devido levando em consideração:
>
> - A extensão do trabalho necessária para alcançar os objetivos do trabalho da auditoria.
> - A complexidade relativa, a materialidade ou a significância dos assuntos aos quais os procedimentos de avaliação (*assurance*) são aplicados.
> - A adequação e a eficácia dos processos de governação, gestão de risco e controlos.
> - A probabilidade de erros significativos, fraudes ou não conformidades.
> - O custo da avaliação (*assurance*) em relação aos potenciais benefícios.
>
> 1220.A2 – No exercício do zelo profissional devido, os auditores internos devem "considerar a utilização de auditoria baseada em tecnologia e outras técnicas de análise de dados.»

Após a análise de tal norma e sendo assim, com o aparecimento desta nova tecnologia de quinta geração as empresas de auditoria e os auditores internos devem estar cientes de que com os aumentos significativos na quantidade de dados em tráfego, estes podem expor qualquer Organização a determinadas situações a ter em conta, tanto a nível financeiro como não financeiro.

Na **Tabela 3.1** constata-se alguns dos parâmetros para os quais a área da auditoria deve estar ciente em virtude do elevado volume de tráfego de dados.

Tabela 3.1 - Problemáticas da adoção do 5G para a auditoria

Tópicos	Definição
Qualidade	Os cargos associados à tomada de decisões necessitam que lhes sejam apresentados/as dados/informações, o mais exatos/as possíveis. Para isso os/as dados/informações devem atender determinados parâmetros normativos de qualidade e cumprir certas especificações relativamente à sua definição e teor.
Conformidade	O não cumprimento dos requisitos de conformidade exigidos pela da ANACOM ou pelo CNCS podem levar à obtenção de penalidades financeiras, de trabalho adicional ou de responsabilidade ao nível social.
Gestão	Os/as dados/informações devem ser meticulosamente bem armazenados/as, através do uso de princípios e processos de gestão de riscos, para que se possa e consiga garantir privacidade, segurança, qualidade e auditabilidade dos/as dados/informações.
Uso desapropriado, desalinhado ou precoce das metodologias	As metodologias de análise de dados/informações são por vezes de difícil aplicação e/ou compreensão e as conclusões retiradas após essa análise precisam de um elevado grau de confiança e para isso são necessários meios e tempo suficiente para uma correta e eficaz gestão, análise e interpretação dos/das dados/informações recolhidos/as.

Ética	A gestão, análise e interpretação dos/das dados/informações recolhidos/as devem estar de acordo com os valores, a missão e a visão de cada Organização bem como alinhadas com os pressupostos para uma correta e fácil tomada de decisão. Devem por isso existir metodologias e determinados controlos ativos para que se possa garantir a recolha, a gestão, a análise e a interpretação ética de todos os/as dados/informações.

Fonte: Autoria Própria

O aparecimento desta nova tecnologia de quinta geração irá tornar a tecnologia operacional muito mais autónoma, isto é, o 5G proporcionará o aparecimento de um tipo de tecnologia capaz de se corrigir pelo aparecimento de alguns *bugs* através de um *checkup* ao seu funcionamento sem que tenha que existir qualquer interferência por parte do homem.

Esta nova automatização na tecnologia operacional aparecerá em diferentes formatos que irão lidar com diferentes desafios e por isso a própria da tecnologia 5G irá provocar algumas alterações, nomeadamente, ao nível da arquitetura das infraestruturas de rede, da segurança, das *clouds*, das análises de *big data*, entre outras.

Conforme indicado na **Tabela 3.2**, o 5G tem três grandes *upgrades* que colocam esta nova tecnologia muito à frente das gerações anteriores de automação:

Tabela 3.2 - Os três grandes upgrades da tecnologia de quinta geração

Upgrades	Definição
Velocidade de navegação	A velocidade de navegação irá aumentar cerca de 20 vezes comparativamente com a tecnologia existente atualmente o que irá tornar a rede de fibra ótica utilizada atualmente numa rede obsoleta e aquém do desejado.
Latência	A latência muito baixa conseguida com o 5G, com cerca de dez milissegundos, irá proporcionar um leque muito vasto e diversificado de novas possibilidades de *feedback* visual e háptico, a comumente chamada de sensação de toque, puramente em tempo real.

Capacidade de conexão	A conetividade melhorará nas áreas rurais que já foram zonas mortas, abrindo mais oportunidades para coletar dados (e prestar serviços) relativos a casas inteligentes, roupas e dispositivos móveis. A conetividade do 5G permitirá uma conetividade confiável e de alta capacidade a uma área maior. Com as normas globais que estão atualmente sendo estabelecidas para o 5G, os trabalhadores móveis terão uma conetividade aprimorada, mesmo quando estiverem a trabalhar no exterior.

Fonte: Autoria Própria

Conceptualmente esta nova rede móvel e tudo o que a ela está agregada, como é o exemplo da TO, mostra-se como uma tecnologia incrível, muito desejada e ambicionada, no entanto, quando for colocada em prática irá certamente levantar questões de segurança e de privacidade. Se os nossos dispositivos eletrónicos estiverem conectados 24 horas por dia e houver a possibilidade de existirem mais dispositivos, configurados com os nossos dados, com a capacidade de se conectarem entre si e/ou à rede, maior será a eventualidade de serem subtraídos por pessoas alheias.

Será por isso, muito importante que a auditoria tome a iniciativa de adotar o mais rápido possível processos de automatização, pois antecipa-se que a era do 5G irá permitir que diversos processos sejam monitorizados e controlados com um nível de precisão nunca antes visto. Tal precisão irá potenciar a alta deteção de problemas como a excelsa prevenção de anomalias a todos os níveis. No entanto pode também por outro lado aumentar o nível de segurança para a entidade para os seus procedimentos e processos.

É por isso fundamental que a auditoria comece já a trabalhar no presente, para o futuro que é amanhã não só para estar pronta para os novos desafios que irão aparecer com o 5G, mas também para que consiga apoiar as entidades a avaliar, compreender e informar o grau em que a TO e a automatização irão afetar as entidades a curto, a médio e/ou longo prazo. Deve por isso, a auditoria, estudar e investigar o *modus operandi* a aplicar para que consiga com o aparecimento do 5G, identificar, avaliar e monitorar os riscos que desta nova tecnologia possam resultar.

Todo este modelo exigirá por parte da auditoria uma abordagem profunda dos trabalhos a realizar, para o entendimento de possíveis novos riscos e da necessidade de se definirem desde cedo mecanismos de controlo bem planeados/delineados, bem como, os próprios auditores reajustarem as suas ferramentas, os seus recursos e os seus mecanismos, para que as mesmas os possam ajudar à prestação dos seus serviços.

Os resultados que os auditores e a auditoria devem estudar, apresentar e conhecer convenientemente com a nova tecnologia que promete ser revolucionária, antes que seja implementada, é pois determinante, para que assim possam ser uns aliados indispensáveis às entidades fazendo-as perceber a forma como os dados são recolhidos, armazenados, analisados e protegidos de forma segura, ao mesmo tempo que, investem em ferramentas, recursos e mecanismos de análise de dados para otimizar e automatizar os novos processos exigidos pela implementação do 5G.

Segundo as normas internacionais para a prática profissional de auditoria interna no *The Institute of Internal Auditors* (The IIA) é possível verificar na norma 2130 intitulada de Controle que:

> «2130 – Controle
>
> A atividade de AI deve auxiliar a Organização a manter controles efetivos a partir da avaliação sua eficácia e eficiência e da promoção de melhorias contínuas.
>
> 2130.A1 – A atividade de AI deve avaliar a adequação e a eficácia dos controles em resposta aos riscos, abrangendo a governação, as operações e os SI da Organização, relativamente a:
>
> - Alcance dos objetivos estratégicos da Organização;
> - Confiabilidade e integridade das informações financeiras e operacionais;
> - Eficácia e eficiência das operações e programas;
> - Salvaguarda dos ativos;
> - Conformidade com leis, regulamentos, políticas, procedimentos e contratos.
>
> 2130.C1 – Os auditores internos devem incorporar o conhecimento dos controlos adquirido em trabalhos de consultoria na avaliação dos processos de controlo da Organização.»

Deve a auditoria por isso, "virar-se" para o tema da Cibersegurança. Desde praticamente o aparecimento da tecnologia relacionada com as redes móveis, que o tema da Cibersegurança e do cibercrime tem sido um risco considerado com um grau de alta prioridade e ao que parece, com esta nova tecnologia, o grau de risco não irá baixar.

Assim, com o aparecimento do 5G, os desafios e os riscos relacionados com a Cibersegurança irão permanecer em constante aumento, uma vez que irão estar em tráfego cada vez mais dados. Está comprovado em diversos artigos e estudos que as práticas de proteção de dados aplicadas no passado, bem como, as atualmente em vigor, não são totalmente eficazes deixando algumas brechas para o cibercrime.

Como resultado, tem havido uma proliferação de novos regulamentos, que lidam com a privacidade e a proteção dos dados, como a Diretiva NIS, a Lei sobre a Segurança Cibernética, o ePR e o conhecido RGPD.

A auditoria pode assim desde já apoiar as entidades a estarem em conformidade com os regulamentos acima mencionados de forma a ajudá-las a entender os procedimentos a realizar para estarem em conformidade, sendo certo que necessita de:

- Se tornar mais ágil;
- Procurar inovação;
- Redefinir processos e ainda,
- Se adaptar.

A auditoria pode assim desempenhar um papel fundamental relacionado com a Cibersegurança. No entanto, para executar tal papel com eficácia, deve haver um vasto conhecimento e um amplo consenso sobre os possíveis riscos inerentes a toda esta nova tecnologia. Tudo isto pode ser alcançado se a área da auditoria mantiver o foco sobre as tendências, for acompanhando as mudanças de acordo com os regulamentos nos trabalhos a executar e se for inovando e adaptando novos processos e controlos.

Os auditores precisam de ser capazes de identificar rapidamente possíveis disrupções e determinar quais dessas disrupções necessitam de um acompanhamento mais próximo e também, quais são aquelas que não precisam de tanta atenção.

Com base neste relato demonstrativo, clarificando a veracidade da investigação relacionado com o primeiro tema (T1) devem por isso ser desenvolvidas estratégias de avaliação de risco, processos de gestão e controlo de mecanismos de automatização. Importa garantir a conformidade com os regulamentos e as normas estabelecidas pelas entidades competentes, incluindo a definição de riscos, proteção de dados, Cibersegurança, automatização e tecnologias operacionais.

T2: Evidências ou falta delas de que o 5G é um real perigo para a Cibersegurança

A veracidade deste segundo tema, passa pela realidade da rede móvel que é um tipo de rede que relaciona atualmente a uma escala mundial, diversos aparelhos tecnológicos, nomeadamente telemóveis e computadores de diversos e distintos utilizadores, transpondo barreiras corpóreas, civilizacionais e ideológicas.

Considera-se irrefutável o seu papel dinamizador no dia a dia das pessoas e empresas, percetível através das vantagens adquiridas em virtude do uso das Tecnologias de Informação e Comunicação (TIC) e da Internet através da rede móvel, sobretudo através de ações realizadas no ciberespaço, em particular, no processamento e tratamento da informação e atualmente através da IoT. Perante esta evidência, é imprescindível a presença por parte das empresas num mundo cada vez mais digital nestas novas redes em prol do seu desenvolvimento, da sua competitividade e da sua inovação num mercado cada vez mais exigente.

Tendo por base o referido anteriormente, foi inevitável o aparecimento de novos desafios que deram origem a díspares ameaças no ciberespaço. Assim sendo, entre elas destacam-se, a propagação de ataques de forma intrusiva aos dados confidenciais das empresas e dos colaboradores destas, o que resultou num incremento acentuado da "espionagem" das ações das empresas, que se refletiu numa perda exponencial de privacidade.

Por tudo isto, a implementação de mecanismos de segurança na tecnologia de rede irá potenciar o atenuar das potenciais ameaças. No entanto, não se deve descuidar a prevenção, a partilha de informação e a formação de profissionais, pois só assim se podem implementar medidas pró-ativas que evitem futuras novas ameaças.

Aferindo a questão presente neste tema é indissociável associar a rede móvel 5G (através da utilização da Internet e todos os seus componentes) agrupando cenários de ciberespaço e obrigatoriamente, aprofundando temáticas relacionadas com a Cibersegurança.

Consequentemente, através da utilização da Internet e dos equipamentos entre si interligados através de aplicações próprias, os utilizadores estarão a desenvolver uma comunicação em rede mais globalizada.

É por isso fundamental que a auditoria possa dominar e compreender o funcionamento da Internet e dos seus serviços, pois um sólido domínio e uma correta e atempada compreensão podem constituir uma mais-valia no reconhecimento de potenciais ameaças à Cibersegurança e na implementação de medidas de mitigação.

Atualmente existem três principais impulsionadores para o registado aumento exponencial e contínuo no volume de tráfego de dados produzidos, no aumento das capacidades de armazenamento de dados e no rápido processamento, análise e produção de dados através da Internet. São eles:

- Computação na *Cloud*[13]
- IoT
- *Big Data*.

Neste alinhamento, o número de aparelhos tecnológicos diversificados conectados entre si e o número de utilizadores com acessibilidade à Internet, têm tornado cada vez mais a tecnologia numa elevada complexidade e com permanentes necessidades de monitorização, vigilância e resiliência.

Desta forma o ciberespaço tem-se tornado numa área com diminuta segurança para a comunicação e partilha de dados, entre outras evidências relevantes. O ciberespaço através da Internet funciona assim como um típico prestador de serviços. Ou seja, a Internet disponibiliza serviços que são executados através de servidores, que recebem e concedem os pedidos efetuados por utilizadores.

Este paradigma de comunicação é designado por Comunicação entre Utilizador e Servidor e é o mais utilizado na Internet com cerca de 8,5 Exabytes (8,5 biliões de Gigabytes) de dados em tráfego[14] diariamente.

É possível verificar na **Figura 3.2**, um exemplo de comunicação entre Utilizador e Servidor, onde a comunicação se inicia através de um pedido feito por um aparelho tecnológico móvel (telemóvel) ao servidor e o servidor por sua vez, dá resposta a esse mesmo pedido. Toda esta comunicação só é possível através de uma rede móvel, neste caso, o 5G.

[13] *Cloud Computing* na denominação anglo-saxónica.
[14] Baseado em dados fornecidos em http://www.Internetlivestats.com/.

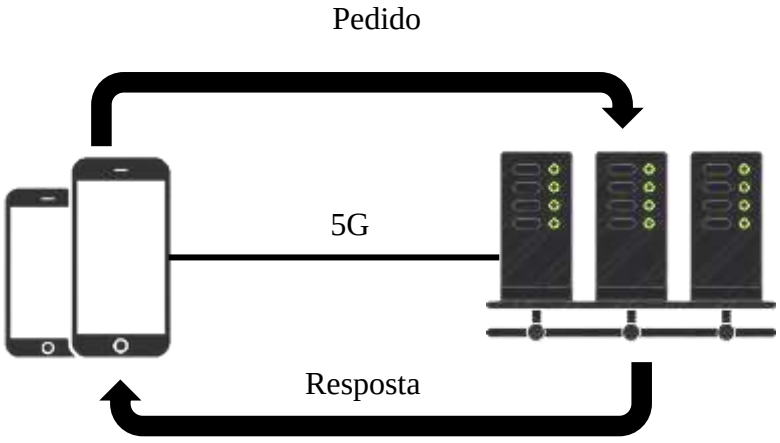

Figura 3.2 - Comunicação entre Utilizador e Servidor
Fonte: Autoria Própria

Em termos práticos, tanto o Utilizador como o Servidor são na prática duas aplicações em execução conjunta, sendo eles, dois terminais distintos (na **Figura 3.2** são um *Smartphone* e um Servidor). Observemos a ilustração da figura acima como um exemplo dos mais comuns nos dias de hoje, o serviço de acesso à Internet.

Tudo começa com o acesso por parte do Utilizador (*Smartphone*) a uma aplicação, tipicamente um *browser* que através de uma "partilha social", conecta-se a uma "página" que estará alojada num determinado Servidor, numa qualquer parte do mundo e por sua vez o Servidor, após processamento do pedido do Utilizador, enviará de volta uma resposta ao mesmo.

Praticamente desde o início deste tipo de envolvimento tecnológico que a comunicação realizada é em grande maioria para a consulta de documentos e o respetivo *download* dos mesmos. No entanto, nos últimos anos em virtude dos três principais impulsionadores mencionados anteriormente está a verificar-se um aumento gradual do *upload* de documentos, muito em virtude da comunicação entre indivíduos e organizações ser cada vez mais frequente. A comunicação é naturalmente ubíqua[15].

A verificação deste aumento deve-se, sobretudo e com um exponencial sem precedentes, à pandemia mundial (COVID-19) que se verificou, em que todos os paradigmas anteriormente disponíveis não previram um aumento gradual e sofreram alterações muito significativas, tornando ao contrário do que era esperado, aumentos consideráveis de *uploads* algo muito utilizado em virtude da subida abrupta do regime de teletrabalho.

[15] Em qualquer lado a partir de qualquer aparelho tecnológico na denominação da gíria popular.

Pelo efeito gerador dos dados submetidos, para além dos já habituais consumidores de dados e de informação do ciberespaço (*downloads)*, passamos a ser produtores assíduos e compulsivos de milhões de dados e informação (*uploads*) que têm de ser partilhados.

A figura seguinte (**Figura 3.3**) tem a intenção de ilustrar esse mesmo facto, anteriormente referido, através da exposição aproximada à atualidade que vivemos do número mundial de *Websites* ativos atualmente e do número total de utilizadores da Internet em todo o mundo.

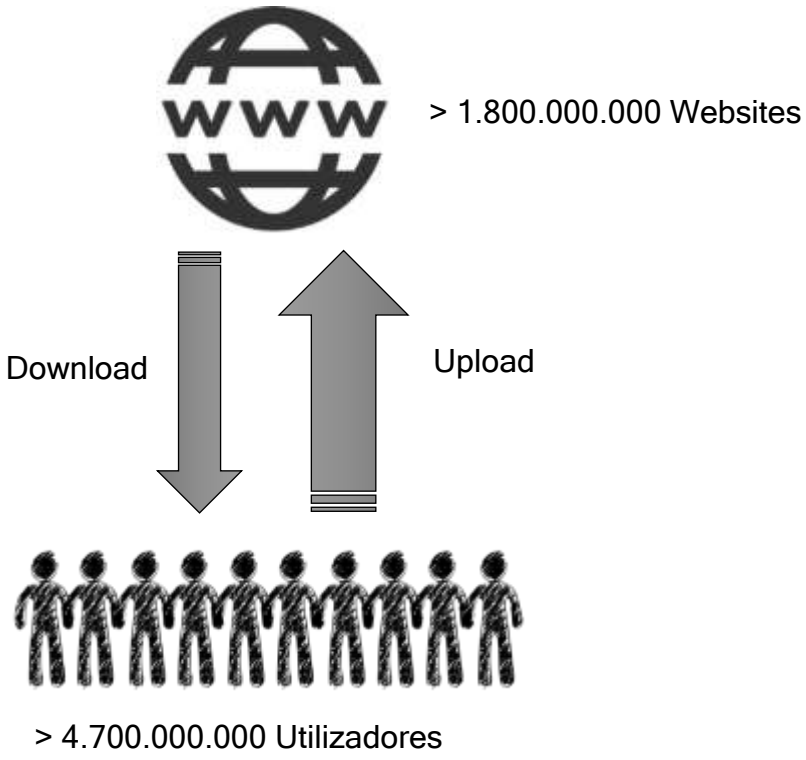

Figura 3.3 - Estatísticas utilizador Internet[16]

Fonte: Autoria Própria

Tendo em conta os picos epidémicos verificados pela COVID-19, que forçaram a obrigatoriedade do teletrabalho, esta tendência de aumento exponencial deverá manter-se tendo em conta o contínuo aparecimento de novas plataformas colaborativas, a incessante aposta nos serviços de *Cloud* e o ininterrupto aumento de aparelhos tecnológicos com a capacidade de se conectarem à rede e gerarem dados de forma continua e autónoma.

[16] Baseado em dados fornecidos em http://www.Internetlivestats.com/.

Sendo assim e com este tipo de comunicação, com o uso massivo da *Cloud* entre outras situações, é ineludível o aparecimento de diversas vulnerabilidades suscetíveis de ataques cibernéticos. Tais vulnerabilidades são sobretudo encontradas nas aplicações e nos sistemas operativos dos utilizadores e no hardware dos servidores, por pessoas/entidades com más intenções com o intuito de provocar danos ou adquirir informações confidenciais.

Tais ataques cibernéticos podem ter diversas formas, seja a partir do acesso remoto não autorizado, através da instalação de programas maliciosos (*Malware)*, à usurpação de informações confidenciais.

Neste contexto, é possível classificar os ataques cibernéticos em dois grupos:

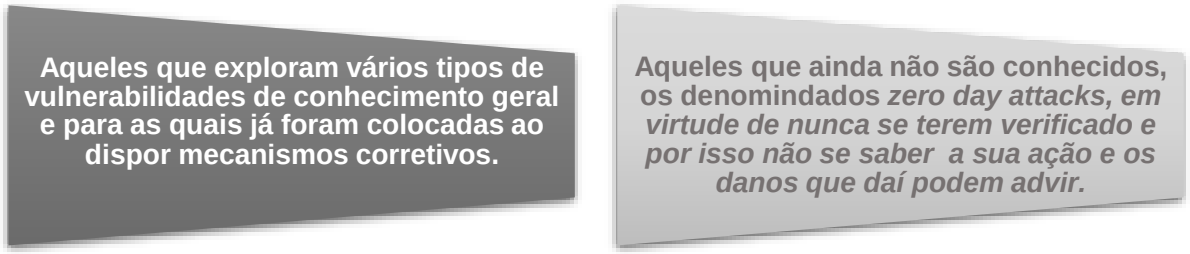

Figura 3.4 - Tipos de ataques cibernéticos

Fonte: Autoria Própria

É assim possível sintetizar alguns tópicos sobre os quais a auditoria deve refletir. Observemos a esse propósito a **Tabela 3.3:**

Tabela 3.3 - Tópicos Gerais de Cibersegurança

TÓPICOS GERAIS DE CIBERSEGURANÇA		
Infraestrutura física	**Protocolos de segurança**	**Documentação pública**
O acesso às infraestruturas físicas associados à comunicação em rede deve ser altamente condicionado, pois é o descuido do acesso a estes locais que muitas vezes permite o saque ou a desativação de componentes destas infraestruturas ou da instalação por meio destes de *malwares* para a obtenção de dados confidenciais.	É necessário que sejam criados protocolos de segurança específicos e detalhados sobre a autenticação e a cifragem da comunicação existente entre utilizador e servidor, pois, é possível que um *hacker* aceda a um determinado servidor e execute ações maliciosas tendo por base o conhecimento geral de um simples protocolo de segurança.	É fundamental que toda a informação crítica e confidencial se encontre em locais de acesso muito restrito e com um elevado grau de segurança e autenticação, porque, informação importante que esteja em local gratuito e de simples acesso torna-se um alvo muito apetecível para a produção de conteúdo malicioso.

TCP

O protocolo de controlo de transmissão é um mecanismo que deveria ser equacionado por todas as entidades uma vez que potencia a segurança das comunicações entre utilizador e servidor. Deveria ser exigido a todas as entidades que as suas comunicações gerassem constantemente certificados digitais com algoritmos criptográficos consistentes.

Serviço *web*

É normalmente associado às comuns e atuais transações comerciais e o pagamento eletrónico com cartões de crédito. Apesar de já ter sido feito muito trabalho para a segurança desta área, ainda existe um mundo infinito na *dark web* que necessita de escrutínio e estudo para uma correta prevenção de possíveis acontecimentos futuros.

MAC e IP *spoofing*

A alteração por parte de um terceiro do Protocolo da Internet (IP) e do Controlo de Acesso a Meios de Comunicação (CAM) para a obtenção de vantagens e de informação confidencial é um tema pelo qual se deveria ter uma maior consideração e atenção, uma vez que é muito utilizado para a clonagem de utilizadores chave.

Aplicações e serviços

Muitas das vulnerabilidades existentes resultam normalmente de erros de desenvolvimento do *software*. São exemplos disso:

- *Buffer overflow* – Acesso a uma parte não protegida de um servidor por parte de um programa externo, podendo ter acesso a informação confidencial.
- *XSS (cross*-site *scripting*) – Execução de *scripts* para a ultrapassagem de controlos de acesso predefinidos, por aplicações em servidores maliciosos, onde é possível visualizar e ter acesso a informação protegida
- *SQL Injection* – Técnica que consiste na submissão de uma mensagem HTTP com bases maliciosas de SQL[17] para o acesso indevido a bases de dados de servidores.
- *Remote access* – Acesso remoto a aparelhos tecnológicos por meio de certas aplicações vulneráveis.

Man-in-the-middle

Man-in-the-middle é o termo técnico utilizado para descrever a ocorrência da invasão por parte de terceiros a uma determinada comunicação entre utilizador e servidor e a alteração desta de forma maliciosa sem que seja detetada a sua presença. Mais uma vez a cifragem toma um lugar de destaque, pois sem esta o conteúdo das comunicações torna-se mais fácil e tecnicamente mais acessível para fins ilícitos.

***Denial of Service* (DoS)**

É a desativação de um serviço associado a um servidor por via do aumento exponencial da quantidade de solicitações feitas ao mesmo. Por cada solicitação efetuada são acionados dois recursos fundamentais em cada aparelho tecnológico. O CPU e a memória. Isso permitirá o colapso dos recursos disponíveis por cada servidor, permitindo a ocorrência de vulnerabilidades.

Fonte: Autoria Própria

[17] *Structured Query Language* – Linguagem utilizada e aplicada em bases de dados.

Para além dos tópicos anteriormente mencionados é ainda de extrema relevância que a auditoria se debruce sobre um tipo de tecnologia cada vez mais em ascensão, a *Cloud*. Observemos a **Tabela 3.4**.

Tabela 3.4 - Tópicos de Cibersegurança na *Cloud*

TÓPICOS DE CIBERSEGURANÇA NA *CLOUD*	
Privacidade O *upload* de dados e de informação na *cloud* têm normalmente riscos associados, uma vez que, os serviços de *cloud* estão associados a fornecedores de serviços e por isso, tudo o que nela for armazenado, passa a ser também propriedade do fornecedor. É por isso de extrema relevância que as entidades entendam que o armazenamento dos seus dados e das suas informações no sistema de *cloud*, acarreta diversos riscos de possível usurpação ou fugas de informação e dados sensíveis.	***Malware-as-a-Service* (MaaS)** Também comum no meio como *Malvertising*, é conhecido como as aplicações maliciosas (*malware*) instaladas nos aparelhos tecnológicos sob a forma de publicidade (*advertising*). Esses *malwares* são normalmente concebidos, preparados e tem a sua localização nas *clouds*, não estando num local físico e estático ao mesmo tempo que coabitam com futuros potenciais alvos, tornando assim o acesso a estes mais fácil.
Redes sociais Foi com o aparecimento destas que a celebre frase "Tudo o que uma vez entra na Internet nunca mais volta a sair" passou a fazer eco nas vidas dos utilizadores. Tudo o que é adicionado às redes sociais (fotos, vídeos, textos, entre outros) é armazenado no servidor online do detentor desta e possivelmente nunca mais é apagado. Existem diversos casos da atualidade que relacionam as redes sociais com fuga de informação privilegiada e privada dos seus utilizadores. A sua utilização acarreta por isso infindáveis ameaças e cuidados a ter.	***App stores*** É fundamental regulamentar o uso deste tipo de "lojas". Trata-se de "lojas" que permitem a instalação de aplicações móveis disponibilizadas pelos construtores de aparelhos tecnológicos. Muitas vezes, para não se dizer sempre, os utilizadores que procedem ao *download* destas aplicações vêem-se confrontados com a obrigatoriedade de autorizarem que os donos da aplicação tenham acesso a um conjunto muito diversificado de dados e de informações armazenadas nestes aparelhos (como por exemplo, contactos, fotografias e localização), bem como a periféricos (as câmaras integradas nos aparelhos). Posto isto, com esta autorização os donos das aplicações passam a ter acesso direto a dados e informações confidenciais e a poderem violar a privacidade dos seus utilizadores de forma consentida.

Fonte: Autoria Própria

Após a análise das duas tabelas anteriores, é percetível aferir que existe uma ampla lista de medidas conhecidas por muitos utilizadores e reguladores que se podem tomar para mitigar total ou parcialmente as vulnerabilidades apresentadas com os tópicos de Cibersegurança.

Na grande maioria dos casos bastará apenas uma mudança de atitude e uma consciencialização dos utilizadores para estas situações, mais recorrentes do que estes pensam e a instalação de aplicações de segurança (como por exemplo *Firewalls*[18], antivírus, sistemas de deteção de instruções[19], entre outros).

A auditoria deve por isso aferir se as entidades estão de acordo com determinados procedimentos envolvendo boas práticas, que poderão minimizar a ocorrência de anomalias e a exposição a vulnerabilidades:

- Se têm instalado e configurado de forma eficiente os seus sistemas operativos e as suas aplicações, de preferência com as últimas versões estáveis e verificar com pessoal informático especializado, como se evita ao máximo a instalação por predefinição e se existe especial atenção e cuidado com os parâmetros relacionados com a segurança;
- Se possuem os equipamentos de comutação, os *routers* e as *switches* parametrizadas com controlos de acesso[20], cujo objetivo reside em fixar regras que permitam aceitar, rejeitar ou bloquear o tráfego vindo de ou com o destino a uma certa rede ou aparelho tecnológico.
- Se recolhem, analisam e interpretam os registos de funcionamento provenientes do servidor, por forma a serem identificadas situações incomuns que necessitem de ser corrigidas. Uma análise atempada e eficiente é fundamental para que se consiga identificar atempadamente a necessidade de intervenção para a prevenção da exposição a riscos desnecessários.
- Se estão implementados diversos níveis de segurança na rede, isto é, se existe uma ou mais *Firewalls* mas também antivírus nos servidores e nos aparelhos tecnológicos com acesso direto à rede.

[18] *Firewalls* são programas que efetuam o filtro do tráfego de rede por vários parâmetros como os endereços IP, endereços MAC ou protocolos aplicacionais.
[19] Sistemas de deteção de intrusões, ou em inglês *Intrusion Detection Systems* (IDS), são programas que utilizam técnicas de deteção de padrões de vírus já existentes e analisam a existência de atividade maliciosa nos aparelhos emparelhados na placa de rede e também nas operações desencadeadas pelo sistema operativo.
[20] *Access Control Lists* (ACL)

São dois níveis de segurança com objetivos muito distintos e diferentes, mas que em conjunto têm um contributo indispensável para um objetivo final e global que é a segurança de toda a rede, dos servidores e dos aparelhos tecnológicos a ela ligados, mas principalmente dos dados e informações nela contidos.

É possível verificar na atualidade do país e do mundo, que o número de delitos com recurso à Internet e a aparelhos eletrónicos têm vindo a aumentar consideravelmente. Com tamanho aumento foi necessário criar leis e diretivas relacionadas com o ciberespaço, a Cibersegurança e o cibercrime.

Foi por isso criado por Portugal em finais do ano de 2011, o gabinete de coordenação destes temas pelo Ministério Publico (MP), vulgarmente chamado de Gabinete do Cibercrime (GC)[21]. Pode destacar-se no Despacho do Procurador-Geral da República[22] os seguintes objetivos do GC:

- A troca de informação e a partilha de experiências entre magistrados do MP, diversos órgãos da Polícia Judiciária ligados ao tema do cibercrime e os prestadores de serviços que potenciem o cibercrime e que a ele estejam ligados através de um fórum permanente;
- A promoção e realização de ações formativas relacionadas com a prova digital para todos os membros participantes no fórum;
- A realização de parcerias com prestadores de serviços para a execução de perícias digitais e para terem acesso total às redes de comunicações utilizadas por estes.

A Lei n.º 46/2018[23], designada vulgarmente por Regime Jurídico da Segurança do Ciberespaço, teve origem para acomodar uma realidade cada vez mais comum no âmbito dos cibercrimes e burlas através de aparelhos tecnológicos. Contudo, esta Lei é do ano de 2018 e com o constante avanço da tecnologia e por consequência do ciberespaço, nem todos os cenários se encontram compreendidos e mapeados.

A **Figura 3.5** ilustra a organização geral da Lei n.º 46/2018. É composta por cinco capítulos, num total de 33 artigos. Os capítulos I e V referem-se respetivamente às disposições gerais e às disposições finais da lei.

[21] Mais informação sobre o GC em: http://cibercrime.ministeriopublico.pt.
[22] http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/desp_pgr_cibercrime_7_dez_2011.pdf.
[23] http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2930&tabela=leis&ficha=1&pagina=1&so_miolo=S

Quanto aos capítulos II, III e IV são os mais relevantes. Neles podemos encontrar os artigos que poderão ser acionados num vasto conjunto de crimes que utilizam equipamentos informáticos. Para estes três capítulos em particular, é apresentada em seguida uma descrição detalhada.

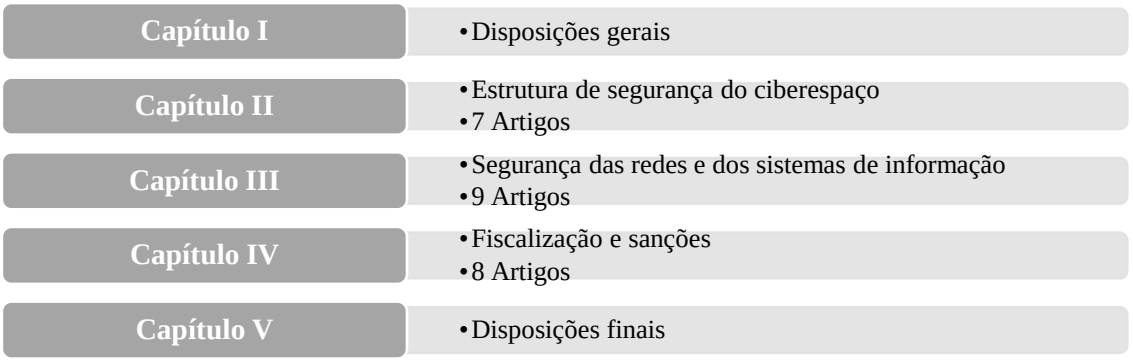

Figura 3.5 - Organização geral da Lei n.º 46/2018

Na **Figura 3.6** ilustra-se a organização dos artigos presentes no capítulo II, apresentando-se uma breve descrição dos seus títulos.

Neste capítulo realça-se as seguintes preocupações do legislador:

- A exposição das definições e composição das entidades responsáveis pela estrutura de segurança do ciberespaço;
- A descrição das competências de cada uma das entidades.

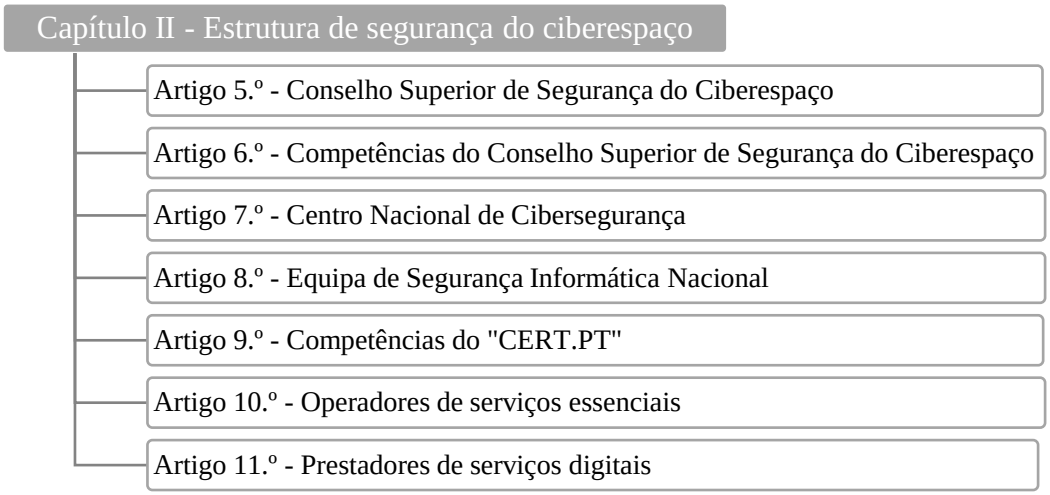

Figura 3.6 - Lei n.º 46/2018 - Capítulo II

Concretamente para o Capítulo III, dedicado à segurança das redes e dos SI ilustra-se na **Figura 3.7**, a sua organização acompanhada de uma breve descrição dos títulos dos artigos.

Relativamente a este Capítulo (III) pode identificar-se como preocupação principal do legislador a definição de requisitos para a preservação, revelação e apresentação dos incidentes.

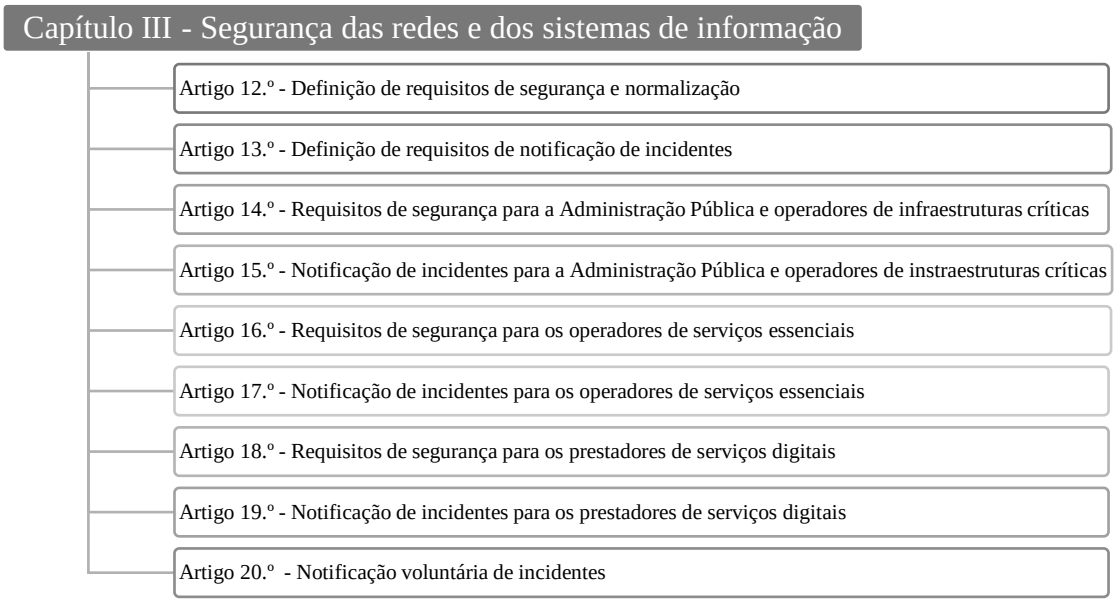

Figura 3.7 - Lei n.º 46/2018 - Capítulo III

Finalmente no que diz respeito ao Capítulo IV, onde são legislados os aspetos relacionados com a fiscalização e as sanções, ilustra-se com a **Figura 3.8** a sua constituição, acompanhada também de uma breve descrição dos títulos dos artigos.

Neste Capítulo (IV) realça-se como principal preocupação do legislador a regulação e regulamentação das contraordenações e a sua distribuição por tipo de contraordenação.

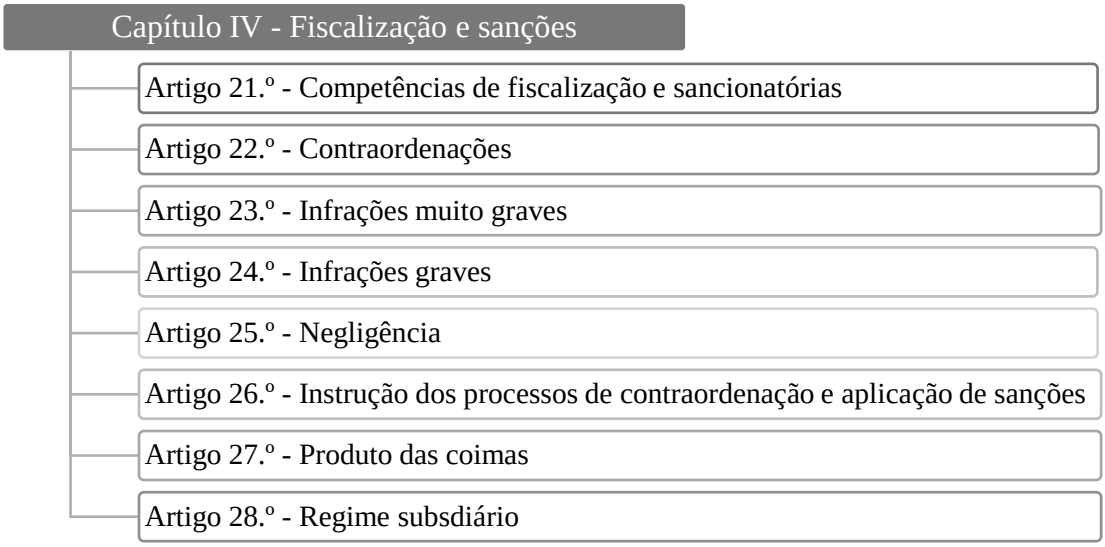

Figura 3.8 - Lei n.º 46/2018 - Capítulo IV

Todavia, apesar do enorme passo que a Internet proporcionou na partilha de informação à escala global, a auditoria deve ter em consideração o que existe por trás desta relevância, em concreto, um vasto leque de ameaças à segurança e integridade dos dados que constante e regularmente são processados.

A auditoria deve por isso ter um sentido de compromisso para com as áreas tecnológicas, nomeadamente, para com a rede móvel de quinta geração, na medida em que são vastos os benefícios que esta trará aos seus utilizadores. A auditoria deverá por tudo o que anteriormente foi exposto, avaliar de forma contínua esta inovadora rede móvel em função dos potenciais riscos a ela associados.

A compreensão do funcionamento desta rede móvel, nomeadamente nos serviços prestados via Internet e respetivas tecnologias relacionadas, sobretudo nos novos e futuros aparelhos tecnológicos em desenvolvimento, a sua utilização e consumo generalizado, constitui um passo muito importante na identificação de potenciais problemas de segurança e na sua mitigação.

Sendo um facto que a tecnologia 5G ainda não pode ser auditada, julga-se relevante o segundo tema (T2) uma vez que se impõe uma clarificação dos tópicos e mecanismos legais apresentados, uma formação adequada aos profissionais envolvidos e de acordo com a problemática na adoção do 5G em futuros trabalhos de auditoria.

T3: Controlo da ASI relativamente a eventuais danos colaterais

É inegável que a antiga versão Internet (1.0) veio simplificar a conexão das pessoas e das coisas globalmente. Já a atual, mas desatualizada versão Internet (2.0) veio possibilitar a produção e a partilha de diversos conteúdos através de cada vez mais aparelhos tecnológicos.

Mais disponibilidade significa mais auditabilidade. Este terceiro tema (T3) depara-se com um conjunto de variáveis como espaço, tempo e realidade virtual que sofrem constantes mutações em virtude da presença massiva das TI no nosso dia-a-dia. As barreiras de espaço são hoje facilmente ultrapassadas, particularmente nos objetos onde é possível a sua desmaterialização, como é o caso da informação, dos documentos e do dinheiro, ao mesmo tempo que, é possível concretizar distintas tarefas com a coadjuvação das tecnologias.

Esta evolução, desde a chegada da Internet ao aparecimento da Inteligência Artificial (IA) e da generalização da IoT, está patente na **Figura 3.9**.

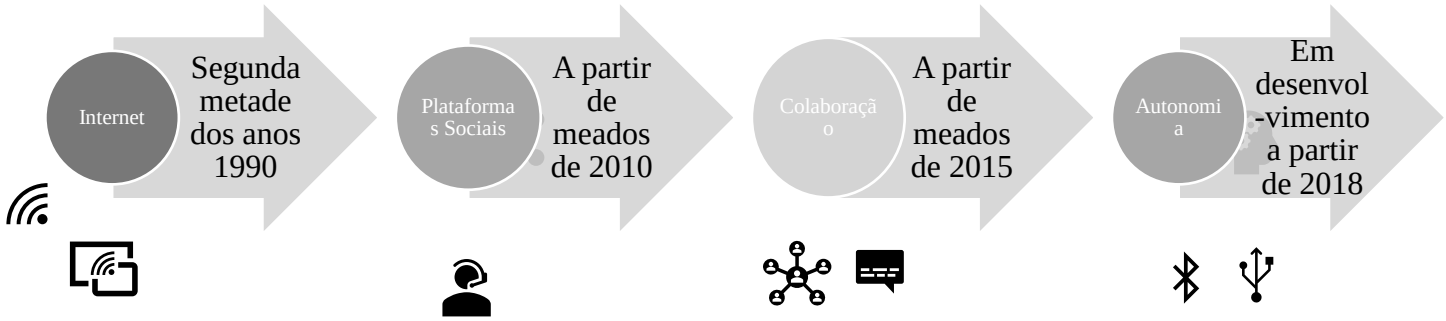

Figura 3.9 - Fases Era Digital

Fonte: Adaptado de *Crowd Companies* (jan. 2016).

Num mundo cada vez mais digital em que vivemos, as TIC assumem um papel central nas nossas vidas, tanto a nível económico como pessoal. Nas Organizações, por exemplo, o lema *Bring Your Own Device* (BYOD) [24] é cada vez mais utilizado, o que leva a uma interação de dados e informação na rede de equipamentos da Organização e equipamentos pessoais e um consequente aumento da complexidade e de segurança.

[24] Traga o seu equipamento pessoal

Toda esta nova dinâmica está a tornar a nossa vida progressivamente e a um ritmo bastante acelerado, cada vez mais digital, por forma da ligação existente entre pessoas e coisas.

Perante estas mudanças tem emergido um tema para o qual a auditoria se deveria debruçar com mais acuidade, a Informação Ambiental[25].

Segundo O'Brien (1990), podemos definir sistema como "um grupo de elementos inter-relacionados ou de elementos interagindo formando um todo" e de acordo com Oliveira (2009) um SI será "um conjunto variado de diferentes e diversa natureza, que, mediante modelos de combinação produtiva, se combinam entre si, com vista à recolha, tratamento, armazenamento e disponibilização de informação".

É por isso um facto que os SI estão cada vez mais interligados e com forte componente tecnológica. A grande maioria de dados e informação, em trânsito, circula nesse ambiente tecnológico.

Uma vez que as fontes de dados e informação são tão distintas e diferentes, as organizações sentem inúmeras dificuldades em geri-los. Existe a necessidade de tratar os dados e a informação a nível operacional, compras e vendas por exemplo, onde são fornecidos elementos no formato desejado, os quais são armazenados em sítios devidamente definidos.

Em pleno Séc. XXI, as organizações também terão a ambição de gerir as vontades expostas nas redes sociais ou nos acessos preferenciais a *apps, websites* e *emails.* É daqui que resultam os dados e as informações não estruturadas e sobre os quais se procuram produzir análises de conteúdo.

A estes dados acrescem os dados fornecidos pela IoT, lidos por diversos aparelhos ou muitas vezes, ativados através de aparelhos eletrónicos que permitem por exemplo, a partilha de localização ao momento. A esta pluralidade, volume de fontes digitais de dados e informação dá-se invariavelmente o nome de *Big Data.*

Mas será assim a informação e os SI algo tão relevante para a auditoria? Entenda-se que é necessária informação para controlar tudo o que nos rodeia. Controlar as horas, a conta bancária, a nossa agenda, ajuda no momento de tomar decisões e até mesmo na definição do melhor momento para agir.

Assim, é de todo relevante que se defina com rigor três conceitos essenciais. São eles: Dados, Informação e Conhecimento. Observe-se a **Tabela 3.5**.

[25]A Informação Ambiental representa todo o tipo de comunicações que recebemos com informação personalizada sobre nós por via da capacidade dos objetos instalados em nossa casa ou nas nossas organizações.

Tabela 3.5 - Os três conceitos essenciais da Gestão do Conhecimento

Conceito	Definição
Dados	São factos/eventos, imagens ou sons que podem ser pertinentes, ou úteis, para o desempenho de uma tarefa, mas que por si só não conduzem à compreensão de determinado facto ou situação (por exemplo, 2500 é um dado) (Alter, 1992).
Informação	Pode ser vista como algo que dá forma ao pensamento, até pelo facto de ser um "objeto formatado, criando artificialmente pelo homem, tendo por finalidade representar um tipo de acontecimento identificável por ele no mundo real, integrando um conjunto de registos ou dados e um conjunto de relações entre eles, que determinam o seu formato" (Le Moigne, 1978). Já de acordo com Lucas (1987), a informação "é uma entidade tangível ou intangível que reduz a incerteza sobre uma dada situação ou acontecimento". Para Oliveira (2009), a informação "é tudo aquilo (...) que aumenta o meu grau de conhecimento ou diminui o meu grau de incerteza, face àquilo que estou interessado em conhecer, intervir ou atuar".
Conhecimento	"É a capacidade de uma pessoa relacionar estruturas complexas de informação para um novo contexto. Novos contextos implicam mudança – ação, dinamismo. O conhecimento não pode ser partilhado, embora a técnica e os componentes da informação possam ser partilhados" (Grenier & Metes, 1992).

Fonte: Autoria Própria

Após análise da tabela anterior e de acordo com os autores, entende-se que os dados são factos registados, recolhidos de várias fontes e a informação é resultado do processamento desses mesmos dados. Toda esta transformação dos dados em informação e posteriormente em conhecimento resulta pura e simplesmente do facto de nós lhes acrescentarmos algum significado, como afirmam Davenport e Prusak (1998).

É possível atualmente ter acesso a informação de cariz pessoal, empresarial, noticiosa, entre outros, em múltiplos aparelhos tecnológicos em distintos locais e por isso, releve-se para a auditoria a revolução que a IA está e irá potenciar num futuro próximo, que está a transformar o paradigma social e onde as ameaças de uma ciberguerra parecem cada vez mais certas, caso não se atue de forma preventiva.

Esta nova realidade insere-nos numa revolução tecnológica, antropológica e civilizacional, que tem vindo a mudar a forma como vamos lidando com a realidade, bem como, a nossa experiência para com o mundo, o que nos caracteriza como uma A Sociedade da Informação[26]. Observe-se a **Figura 3.10**, onde são exemplificadas as dimensões éticas da Sociedade da Informação.

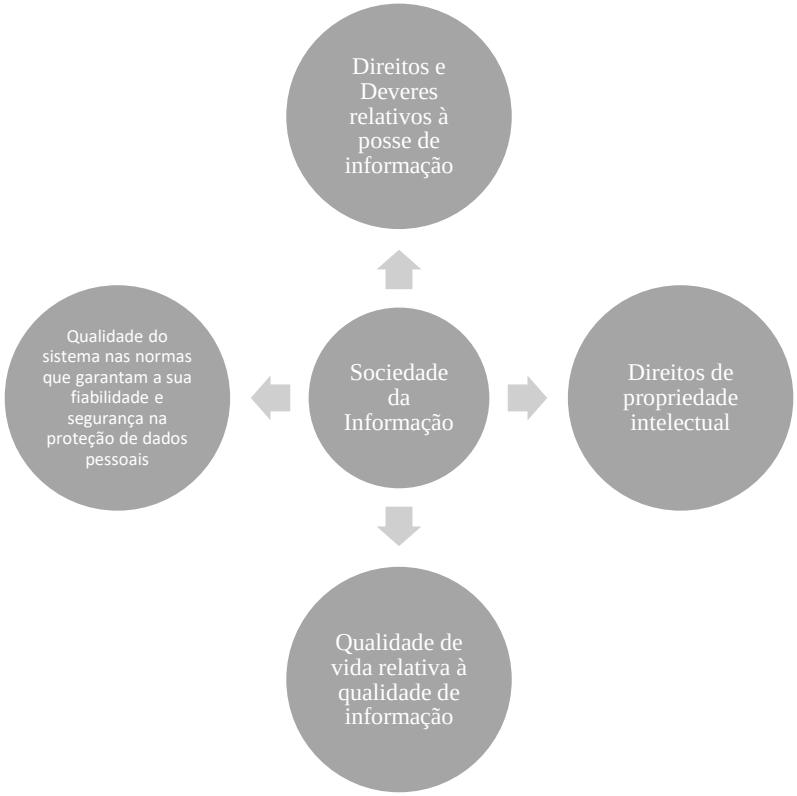

Figura 3.10 - Dimensões éticas da Sociedade da Informação

Fonte: Autoria Própria

Esta é por isso uma sociedade de estreita relação com as dimensões éticas, sociais e políticas que têm vindo a assegurar o direito à informação e à responsabilidade no seu uso, garantindo a todos os utilizadores a desejada qualidade de vida no que diz respeito à privacidade, sem que estejam comprometidos os níveis de segurança em causa com este tema.

[26]A Sociedade da Informação é uma sociedade interligada, flexível, participativa, móvel, criativa, onde a informação e o conhecimento são gerados e partilhados em ambientes cada vez mais mediados pela tecnologia.

Estará a auditoria preparada para uma sociedade cada vez mais moderna, repleta de dados e informações disponíveis a terceiros por meio de uma transação, de um simples telefonema, da interação com um aparelho tecnológico, ou de um acesso básico a uma página eletrónica, que podem ser relacionados e cruzados em frações de segundos por meio de uma simples pesquisa em diversas bases de dados onde estes estão disponíveis?

Esta evolução tecnológica que permite a organizações ou a *hackers* usufruírem da máxima *everything everywhere*, com base na falta de controlo e de regulação, à violação da esfera da privacidade da vida pessoal e privada de diversos utilizadores.

Deve por isso a auditoria estar envolvida no desenvolvimento de portais eletrónicos e de *websites*, a fim de se evitar o uso de informação que possa violar os direitos de propriedade dos seus utilizadores. O desenvolvimento e a anatomia dos portais eletrónicos e dos *websites* podem, eventualmente, revelar o uso indevido de logótipos, o uso de texto, o uso de imagens, ou o uso de artigos sem a devida autorização e/ou sem a identificação do autor.

Para a aplicação de procedimentos dos SI a auditoria deve criar procedimentos de controlo baseados em barreiras físicas, em acesso por controlo biométrico e em comunicações de segurança por meio alternativo. Observe-se a **Figura 3.11** onde são explicadas tais políticas.

Figura 3.11 - Políticas de Controlo SI

Fonte: Autoria Própria

Para dar apoio a esses controlos, foi a 25 de maio de 2018 colocado em vigor o RGPD em Portugal, o qual veio legislar, recomendar e obrigar todo o tipo de entidades (públicas ou privadas) a adotar e a aplicar as medidas nele constantes.

Como já mencionado anteriormente no Capítulo II "Enquadramento Teórico", o RGPD vem definir regras de proteção, tratamento e circulação de dados pessoais nos países presentes na UE, bem como, para os países não pertencentes à UE, mas que tratem de dados de pessoas aqui residentes.

Observe-se agora a **Figura 3.12**, onde são espelhadas as principais obrigações do RGPD.

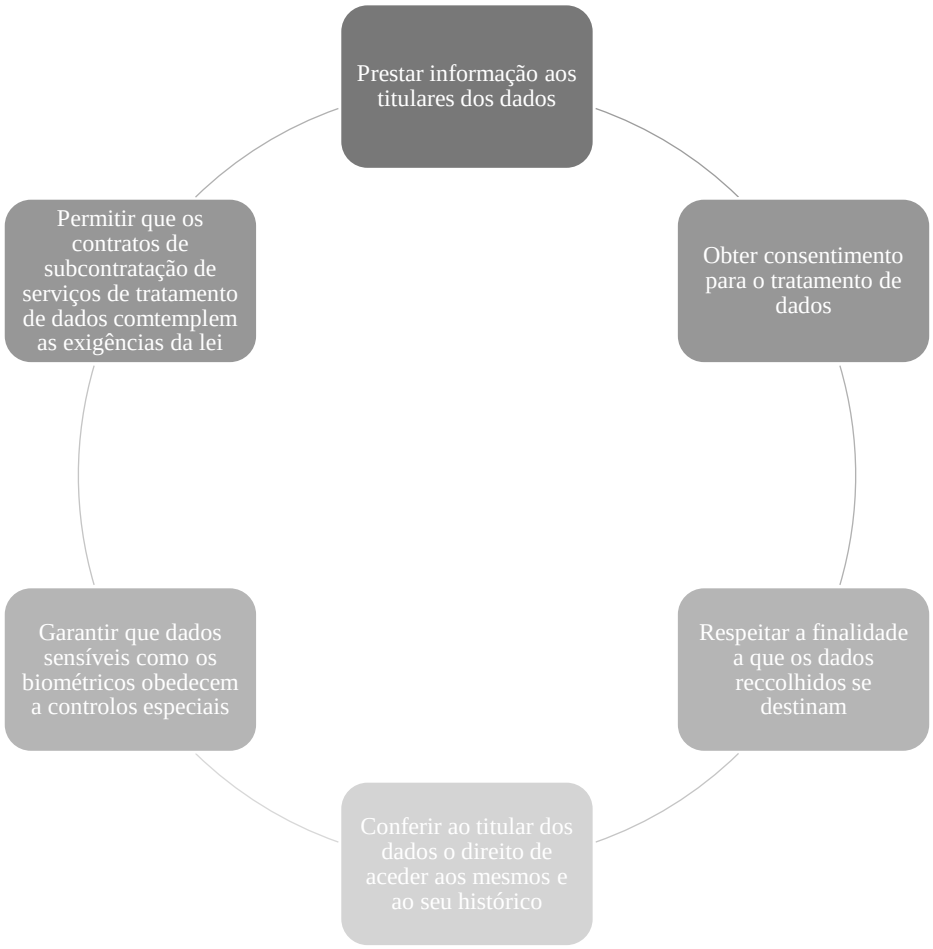

Figura 3.12 - Principais obrigações do RGPD

Fonte: Autoria Própria

O permanente crescimento da dependência das TI e dos SI deparam-nos com novos paradigmas. Entre eles:

1- Atualmente, a informação deixou de existir apenas para atuar sobre a tecnologia e passou a ser efetivamente a sua matéria-prima principal.

2- A importância da informação é de forma inequívoca indiscutível, uma vez que, a informação faz parte de toda e qualquer atividade da sociedade. É por isso de máxima urgência a sua salvaguarda, em virtude de ser tão relevante e necessária para o controlo e tomada de decisões.

3- Por fim, a enorme versatilidade e a tremenda potencialidade da possibilidade de estruturação em rede de toda a informação, já provadas, devido à sua morfologia que se tem mostrado capaz de dar resposta à crescente complexidade da interação desta sociedade.

Com tamanha e abrupta evolução o uso de *Smartphones*, portáteis e outros aparelhos tecnológicos ligados em rede, deixou de ser em função do local onde estes se encontram. Aviões, comboios, automóveis e espaços públicos são transformados nos dias de hoje em locais de trabalho.

É importante que a auditoria tenha em atenção tamanha ubiquidade por parte deste tipo de tecnologia que todos os dias emerge e ganha importância. Nomeadamente, no que concerne à sua universalidade, que permite aceder a todas as redes em todos os locais, à sua exclusividade, que providencia informação personalizada a cada utilizador, ao seu equipamento e ao contexto em que este se encontra (lugar, tempo...) e à sua característica unissonante de multiplataforma que sincroniza e replica informação entre aparelhos tecnológicos de forma muito eficiente, como é o exemplo da *Cloud* e do *Software as a Service* (SaaS). É por isso que os SI à semelhança de qualquer outro sistema têm de ser seguros, não só ao nível de infraestruturas tecnológicas, mas também ao nível muito particularmente do comportamento humano.

Os SI à semelhança de qualquer outro sistema, podem sofrer acidentes pela intervenção humana. Na **Tabela 3.6** são apresentados alguns tipos de erros.

Tabela 3.6 - Tipos de erros nos SI

Tipo	Definição
Entrada incorreta de dados	Por vezes as tabelas das bases de dados veem o seu conteúdo corrigido por instruções lógicas dadas através de *queries*, ou seja, perguntas feitas ao próprio Sistema de Gestão de Bases de Dados (SGBD). Por exemplo, uma pequena alteração do valor em dívida de propinas aplicável a todos os alunos por causa da COVID-19. Se a instrução estiver errada e o colaborador não se aperceber, o impacto pode ser grave ou até gerar cobranças indevidas.
Desempenho do colaborador	Tipicamente ocorre quando este realiza operações com dispositivos individuais e instala atualizações de software que tenham impacto sobre dados locais, acolhendo, por exemplo, vírus e similares.
Omissão de novos procedimentos	Por vezes, os colaboradores agem por conta própria, ignorando procedimentos e recomendações.
Realização e verificação de cópias de segurança	Cópias de segurança que não são feitas ou não se verificam os backups periódicos com recurso a *restore*. Trata-se de aferir se estão a ser aplicadas as regras em termos de segurança informática e que foram aprovadas.

Fonte: Autoria Própria

Para além destes incidentes, é sempre possível que ocorram outros por força da natureza e/ou catástrofes, por exemplo, incêndios. Para estes eventos naturais e para os quais não temos como evitar a sua ocorrência, os locais onde estão instalados os servidores e os sistemas de *backups* devem conter sempre dispositivos altamente sofisticados, prontos a atuar caso sejam necessários.

Por outro lado, existe ainda a possibilidade da ocorrência de erros intencionais, como é o caso da sabotagem. Atente-se aos seguintes casos da **Tabela 3.7**.

Tabela 3.7 - Tipos de sabotagem aos SI

Tipo	Definição
"Bomba-relógio lógica"	Os colaboradores que tenham "saído contra a sua vontade" da empresa, podem deixar pequenos problemas, com intuito de criar danos na Organização.
"Porta das traseiras"	Os colaboradores podem, por motivos do foro financeiro ou pessoal, deixar aberto o acesso a aplicações para testes que pode servir para intervir posteriormente de forma maliciosa contra a Organização.
"Receio de substituição"	Os colaboradores podem ainda sabotar novos sistemas como receio de serem substituídos por um novo software, tentam mostrar que o antigo, ou a sua pessoa, são imprescindíveis ao serviço da Organização.

Fonte: Autoria Própria

Por fim, mas não menos importante, o vandalismo é outra grande ameaça que recai habitualmente sobre *Hardware*[27] e *Software*[28] e que em muito afetam o seu desempenho. Ao falar de vandalismo, inclui-se o roubo físico ou eletrónico, com o intuito de se efetuarem cópias dos dados existentes nestes de forma ilícita. Muitos destes dados, não se encontram encriptados e são normalmente roubados através da técnica *Ransonware*[29]. Com o avançar da tecnologia outras técnicas têm vindo a crescer, nomeadamente a técnica *Key Loggers*[30] e o *Fishing*[31].

Deste modo, a auditoria deve verificar a adoção por partes das organizações de políticas, procedimentos e recursos técnicos de segurança, com o intuito de impedir organizações e terceiros que tenham acessos não autorizados e que alterem, furtem ou provoquem danos nos SI. Um correto e eficaz conjunto de medidas e procedimentos de controlo pode garantir que informações e dados estejam o mais salvaguardados possível.

[27] Servidores, routers, redes, entre outros.

[28] Aplicações, websites, entre outros.

[29] Já referida na subcapítulo 2.2.6 Impactos das Redes Móveis na Empresas. Trata-se na prática do roubo de dados com pedido de resgate para os reaver.

[30] Técnica capaz de capturar o que é digitado no teclado, como passwords ou números de cartão de crédito.

[31] Técnica que consiste em enganar os utilizadores, guiando-os para sites de serviços falsos, fazendo-se passar por genuínos.

Nesta sequência é importante que a auditoria tenha perceção que a vulnerabilidade dos SI resulta da sua infraestrutura em rede, com padrões conhecidos dos especialistas, de erros de configuração, sejam da rede, sejam dos servidores e de erros de instalação, programação ou parametrização não autorizada.

Acresce a tudo isto, a especial vulnerabilidade de acesso por parte dos utilizadores a redes *Wi-Fi* abertas, onde circulam cada vez mais programas concebidos para recolherem dados de acesso privado e restrito. A auditoria deve informar-se acerca destas ameaças, nomeadamente estudar, os vírus informáticos[32], que infetam diariamente milhares de SI, seja através de downloads, seja através da abertura de anexos em *e-mails* de origem duvidosa, os *Worms*[33] e os *Trojan Horses*[34].

Assim é imprescindível que a auditoria, incentive e implemente nas organizações, políticas de utilização de *software* seguro, atualizado, licenciado e corretamente aplicado/instalado, em conjunto com um seguro, atualizado, licenciado e corretamente aplicado/instalado antivírus. É imperativo também que o acesso a aparelhos seja feito através de credenciais intransmissíveis, de modo que cada utilizador só consiga fazer na rede e no sistema aquilo a que o seu perfil tiver permissão para fazer.

Por tudo isto é fundamental que auditoria aplique e faça aplicar as políticas de segurança, com planos de *Disaster Recovery*, que permitem identificar quais os sistemas mais críticos e que podem comprometer a continuidade dos objetivos do utilizador.

Perante o T3 formulado "Controlo da ASI relativamente a eventuais danos colaterais" admite-se o pressuposto desta veracidade, rejeitando-se em termos empíricos cenários transversais, como por exemplo manipulação de dados incluindo-se atividades conhecidas como *Fake News*, pelo que se aceita na generalidade este tema.

[32] Os vírus informáticos consistem em programas que se ligam a ficheiros ou outros programas para serem executados em máquinas alheias e atingirem o seu fim.
[33] Programas independentes que se autocopiam entre computadores através da rede.
[34] Programas dissimulados que se escondem em supostas funções que, de facto, não são as esperadas.

Capítulo IV – Análise de Resultados

4.1 O 5G, a Cibersegurança, os SI e a Auditoria

Assente nas evidências demonstradas e aceitação dos temas formulados, sendo a evolução tecnológica cada vez mais rápida, principal e nomeadamente, no que concerne ao aparecimento de novas redes móveis através das funcionalidades da Internet, a generalização da sua utilização é matéria relevante. Somos hoje assumidamente uma Sociedade da Informação e do Conhecimento, isto é, uma sociedade caracterizada pela rápida partilha e pelo fácil acesso a todo o tipo de informação, aplicando filtros para gerar mais conhecimento.

Por via do armazenamento de toda esta informação ser feito no ciberespaço, o controlo dos acessos à mesma torna-se muito difícil devido a tamanha amplitude, o que está a tornar a informação privada e confidencial mais acessível a piratas informáticos, deixando os seus proprietários vulneráveis a ciberataques.

Após a descrição dos três temas formulados em matéria de 5G, Cibersegurança e SI, com o óbvio aumento dos cibercrimes, os objetivos apresentados nesta dissertação têm, salvo melhor opinião, uma enorme relevância na comunidade, relevância essa que necessita ser acompanhada na área da auditoria. O posicionamento dos profissionais deve ser feito através de mecanismos e procedimentos mais robustos por forma a mitigar ou mesmo reduzir significativamente, tais imperativos tecnológicos na sociedade.

Com base na exposição realizada anteriormente, após a análise dos temas apresentados e formulados, sendo a própria auditoria a este tipo de tecnologia algo muito "abstrato" no que concerne à ASI, apresenta-se de seguida um possível processo de auditoria ao 5G, à Cibersegurança e aos SI, através de uma notação BPMN (**Figura 4.1**), que poderá futuramente ajudar as equipas de auditoria a planear a ordem de trabalhos a desenvolver.

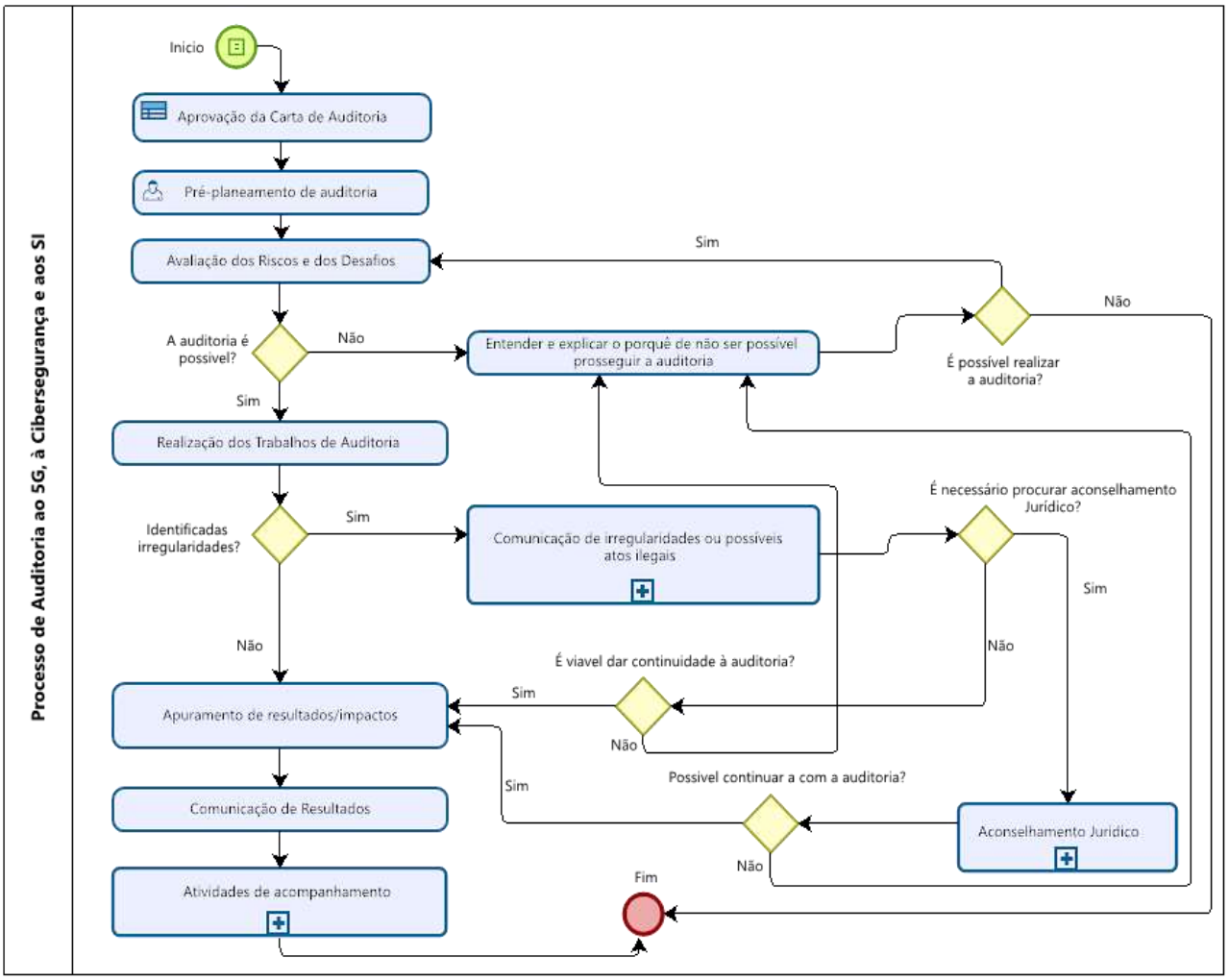

Figura 4.1- Notação BPMN de um possível processo de auditoria ao 5G, à Cibersegurança e aos SI
Fonte: Autoria Própria

4.1.1 Auditoria à recolha de dados com o 5G

A evolução da rede móvel, nomeadamente o 5G, irá suscitar novos desafios para a sociedade, especificamente, ao nível da Cibersegurança e da proteção de dados.

Sendo a Cibersegurança e a proteção de dados, dois temas atuais, a auditoria uma vez mais tem a obrigação de se adaptar a novas realidades, dotadas de mecanismos baseados na tecnologia, especialmente na TO, em conjunto com outras técnicas de análise de dados.

Um alinhamento a processos de negócio é imperativo. O objetivo é modelar e simular métodos que incutam às organizações medidas corretivas, aptas para a preservação e a segurança dos dados recolhidos, sendo ao mesmo tempo capazes de garantir à auditoria um maior grau de segurança e confiança. De modo geral e como se procurou desenvolver ao longo da presente dissertação,

> «[…] Se os nossos dispositivos eletrónicos estiverem conectados 24 horas por dia e houver a possibilidade de existirem mais dispositivos, configurados com os nossos dados, com a capacidade de se conectarem entre si e/ou à rede, maior será a eventualidade dos dados serem subtraídos por pessoa alheias»,

as dificuldades para o controlo de dados em trânsito e para uma correta análise destes aliados a uma rede muito superior ao existente atualmente serão inúmeras. Terá assim a auditoria de estar em constante atualização relativamente aos SI e TI, independentemente do seu grau de complexidade relativamente à Cibersegurança e à proteção de dados. Por tudo isto, é impreterível difundir o estudo e o conhecimento, bem como, a conformidade com as obrigações legislativas em vigor, como por exemplo as leis que ao longo desta dissertação foram referidas, a Diretiva NIS, a Lei sobre a Segurança Cibernética, a ePR e o RGPD.

Deste modo, a auditoria ganha um papel muito relevante relacionado com a Cibersegurança. A auditoria depara-se com um novo paradigma, na medida em que se torna imprescindível a realização de auditorias em analogia com esta matéria, capazes de estabelecer mecanismos de controlo adequados de modo a assegurar a conformidade e a segurança na recolha, análise e utilização de dados por parte das organizações.

Perante esta exposição, quaisquer trabalhos de auditoria relacionados com esta matéria, os mesmos devem ser iniciados através de uma preparação técnica através da recolha de diversas informações relativas aos ambientes informáticos da Organização em causa, por forma a reunir-se o conhecimento necessário para um correto compromisso da auditoria. Releva-se por isso imperativo compreender o comprometimento da Organização para:

I) A recolha e armazenamento de dados;

II) A segurança dos dados recolhidos;

III) O grau de utilização das novas tecnologias;

IV) O conhecimento da nova tecnologia de rede móvel, em concreto, o 5G.

Assim sendo, a área da auditoria deve preocupar-se com algumas questões, com as quais se irá deparar num futuro próximo aquando da auditoria a este novo tipo de tecnologia. De seguida na **Figura 4.2** é possível identificar algumas questões pertinentes, em antecipação, para que a auditoria se adapte a esta nova realidade e verificar se as organizações estão em conformidade com os regulamentos afetos à Cibersegurança.

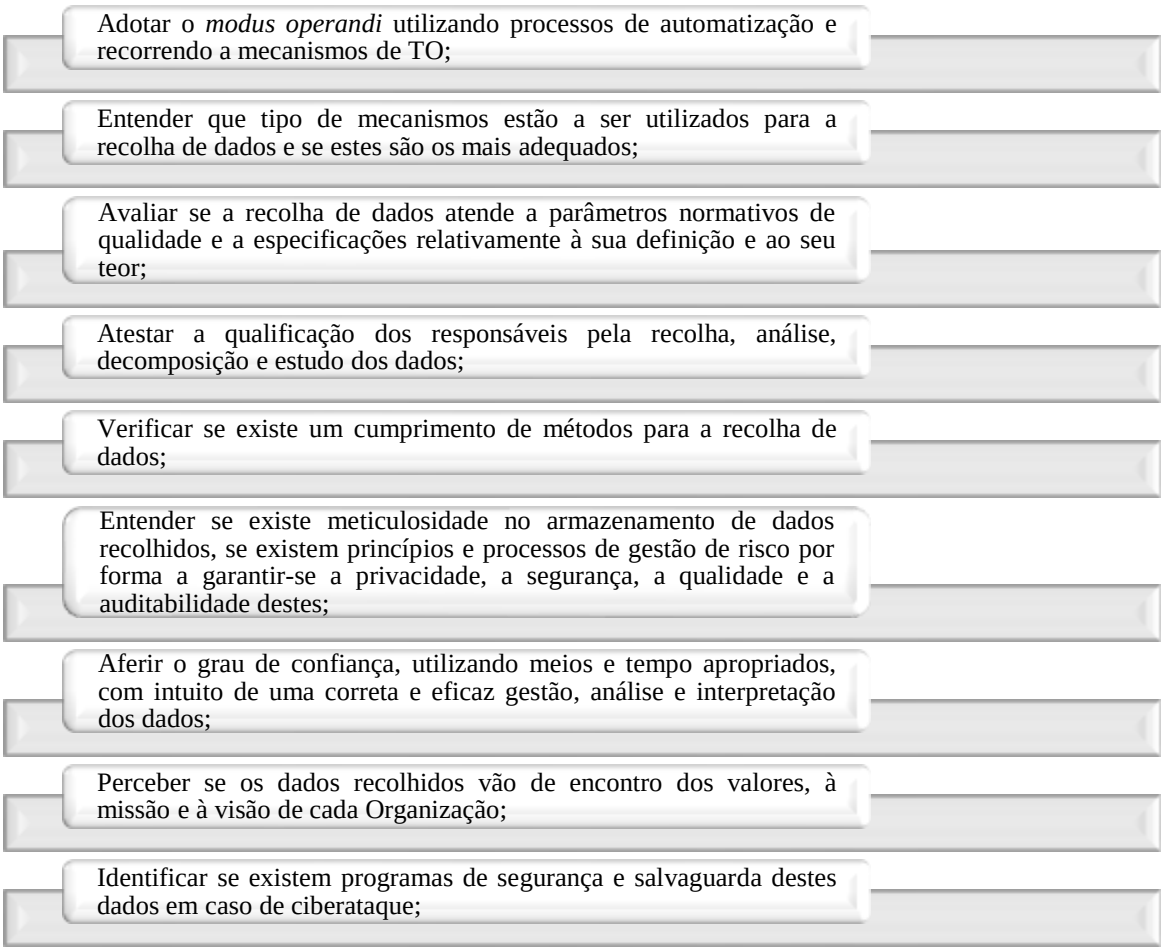

Figura 4.2 - Questões sobre a auditoria à recolha de dados com o 5G

Fonte: Autoria Própria

Estas questões como anteriormente já referido, embora tenham sido feitas numa fase empírica de investigação, são bastante pertinentes tanto para a auditoria como para as organizações, uma vez que espelham preocupações reais a ter num futuro muito próximo.

Posteriormente, para os novos planeamentos a fazer antes de um trabalho de auditoria na área de SI com para qualquer outra área, deverá ter-se em consideração um conjunto de ferramentas e uma sequência de metodologias que tenham a capacidade de dar resposta aos novos desafios impostos pela nova realidade.

Sucintamente, o 5G será uma mais-valia para a Sociedade de Informação e do Conhecimento e é apenas um começo da enorme complexidade em que a área da auditoria estará envolvida, no sentido em que se traduz numa realidade totalmente, ou ainda muito desconhecida, que ao mesmo tempo necessita urgentemente da implementação e de novas metodologias.

4.1.2 Auditoria à Cibersegurança

Será que existe Cibersegurança sem a ocorrência de auditorias? Entenda-se que a Cibersegurança é uma condição que se pretende garantir e manter e que é normalmente caracterizada pela ocorrência de eventos adversos nas redes e nos SI que põem em causa a segurança esperada.

Sendo a auditoria uma área dedicada ao auxílio a empresas com o intuito de mitigar os riscos existentes e na deteção de possíveis inconformidades, é fundamental que esta consiga identificar as inconformidades que possam a vir a requerer uma ação corretiva ao nível de ataques intencionais, violações, incidentes, bem como, às respetivas consequências que advenham destes.

Neste contexto, a auditoria tem uma função preponderante relativamente à Cibersegurança, pois pode identificar quais os dados e as informações, que são de facto relevantes e quais destas podem ser mais suscetíveis a roubo.

A auditoria deve por isso avaliar o controlo e a segurança nos acessos a esse tipo de dados e informações, bem como, aos SI onde são armazenadas.

Observando a atual conjuntura, onde a grande maioria das empresas se viu obrigada a alocar os seus recursos a trabalhar à distância, nomeadamente o teletrabalho ou o trabalho à distância, a segurança das plataformas informáticas e dos SI assumem ainda mais relevância.

Segundo dados estatísticos fornecidos pela ANACOM, o serviço de internet fixa e móvel aumentou cerca de 61,1% (ANACOM, 2020), muito em virtude das medidas de combate em fase de pandemia. Estas circunstâncias favoreceram naturalmente o aumento de ameaças e riscos associados à Cibersegurança.

Observe-se a **Figura 4.3**, retirada do site da ANACOM, onde são espelhados alguns dados estatísticos relativamente ao aumento exponencial do tráfego de dados e de Internet móvel relativamente ao 3.º trimestre de 2020, período referente às férias e o regresso ao trabalho (numa conjuntura de teletrabalho) da maioria da população portuguesa.

Figura 4.3 - Serviços Móveis - 3T2020

Fonte: Autoridade Nacional de Comunicações

Tendo em consideração que mundialmente o crescimento foi igual ou superior ao ocorrido em Portugal, foi identificada a subida das ciberameaças relacionadas com a COVID-19, nomeadamente, campanhas de *Phishing*, *Ransonware*, aplicações fraudulentas, desinformação, fraudes digitais, entre outras.

Considerando ainda os dados apresentados, é notório que existem vários aspetos a melhorar sobretudo, no que diz respeito às atitudes e ao comportamento dos utilizadores que se posicionam cada vez mais no ciberespaço.

Por si só, a Cibersegurança é um desafio complexo de se gerir. Evidentemente, sendo o *Phishing* e o *Ransoware* os dois principais riscos associados à Cibersegurança, é importante que se estipule por parte da auditoria o que se deve fazer para se prevenir futuros incidentes, promovendo a passagem da atitude ao comportamento, para lá da preocupação ou da reação, isto é, a auditoria deve promover a construção de uma estratégia clara para a resiliência do ciberespaço, num tempo em que este ganha uma importância cada vez mais acrescida.

É preciso, por isso, assegurar que os controlos internos são robustos e estão corretamente implementados, bem como, a formação específica e correta dos utilizadores das informações mais relevantes. É preciso ainda que exista determinada consistência[35] técnica, necessária para proteger as entidades das tentativas de ataques cibernéticos, cumulativamente com um plano de recuperação de desastres (*disaster recovery*) definido e preparado para entrar em prática de forma rápida e eficiente, caso seja necessário.

Com o atual panorama de contínua mudança, agregado ao desenvolvimento tecnológico e das suas plataformas com o aparecimento de novas ameaças, a auditoria depara-se com novos desafios relacionados com a aprendizagem de novas competências principalmente na área da engenharia informática e com a obtenção de novas certificações que permitam a adoção e utilização de metodologias inovadoras, bem como, a aquisição de um conhecimento alinhado com as dinâmicas empresariais.

4.1.3 Auditoria aos SI (ASI)

Todas as entidades deveriam proceder à elaboração de auditorias periódicas aos seus dados e aos seus SI, uma vez que os SI são a representação cibernética de diversos elementos físicos de cada entidade, onde não se podem separar fatores sociais de fatores técnicos e onde se conjugam diversas componentes entre elas o hardware, o software, os dados, os processos e pessoas, de modo a que se consiga criar, armazenar e distribuir informação útil e relevante como componente fundamental para a tomada de decisão e delineamento da melhor estratégia.

Neste contexto, a ASI apresenta-se como uma mais-valia que tem como intuito auxiliar as entidades nomeadamente:

- A lidar com a mudança imposta pelos fatores externos à entidade;
- A análise das tendências e ainda,

[35] *Awareness* em termos técnicos.

- A otimização do desempenho dos SI.

Esmiuçando os temas já formulados e que foram aceites em termos empíricos, é pertinente aprofundar os conhecimentos relacionados com os trabalhos de auditoria para dar às entidades a nível dos SI, uma clara identificação de aspetos a melhorar no SI e assim conseguir fundamentar decisões estratégicas que as tornem competitivas e que as façam crescer apesar das envolventes em que se inserem.

Espera-se também que após uma ASI as entidades tenham as suas operações avaliadas e validadas ao nível da qualidade, designadamente, se estão enquadradas com a evolução digital e o impacto/risco desta na entidade.

Para isso é impreterível que as equipas de auditoria sejam multidisciplinares para que o conhecimento desta área seja o mais completo possível, sobretudo ao nível das competências informáticas, uma vez que, estas são nos dias de hoje cada vez mais uma mais-valia e que devem ser aliadas ao já existente espírito crítico e analítico na área da auditoria, dada a crescente complexidade dos SI disponíveis e da informação e dos dados que contêm.

Na **Figura 4.4** enumeram-se algumas *frameworks* de referência para a ASI.

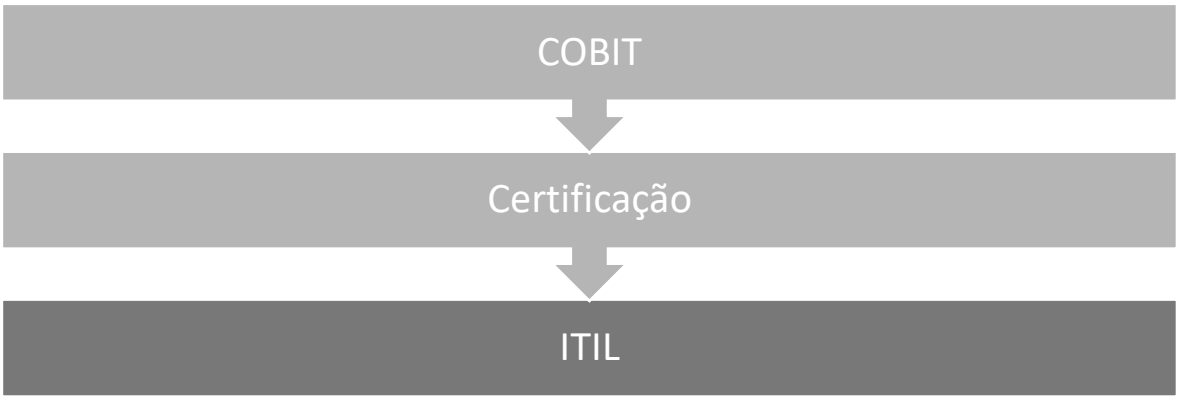

Figura 4.4 - *Frameworks* de ASI

Fonte: Dissertação Auditoria dos Sistemas de Informação das Instituições Financeiras, Martins, Ivan, ISCAL

A missão do modelo COBIT é definido pelo ISACA[36] como sendo «pesquisar, desenvolver, publicar e promover um modelo de controlo para a governança de tecnologias de informação atualizado e internacionalmente reconhecido para ser adotado por organizações e utilizado no dia-a-dia por gestores de negócios, profissionais de tecnologias de informação e profissionais de avaliação». É possível ainda afirmar que os 4 principais atributos do COBIT são o foco no negócio, a orientação nos processos e nas medições e a base nos controlos.

Já ao nível de certificações, as normas ISO 27001 e a ISO 9001 são as mais procuradas. A ISO 27001 está associada à gestão da segurança de informação elaborada para as empresas e a ISO 9001 está associada os mecanismos de implementação de um sistema de gestão de qualidade, igualmente orientada para as empresas.

Estes normativos permitem que uma Organização tenha os seus processos e serviços certificados por meio de uma avaliação externa que pode acrescentar valor à Organização, desde que estejam em concordância com determinados requisitos constantes nas normas internacionais ISO.

Em regra, as certificações ISO são feitas por imposição comercial e técnica, obrigatória e legal para a comercialização de determinados produtos e serviços a clientes. As auditorias realizadas permitem atribuir (ou não) às empresas um certificado que garante conformidade com determinados requisitos.

Por fim a ITIL[37] reúne um conjunto de mecanismos e ações no que aos serviços de TI dizem respeito para a sua efetiva melhoria contínua.

[36] *Information Systems Audit and Control Association*
[37] *Information Technology Infrastructure Library*

Capítulo V – Considerações Finais

Num momento em que o 5G é um dos temas de discussão com maior destaque num âmbito tecnológico, devido a todas as novidades aguardadas, todas elas muito aliciantes tanto para o mercado laboral como pessoal. Neste último capítulo será apresentada de forma sistemática a relação existente entre o estudo empírico realizado, a análise efetuada através da revisão bibliográfica e os temas sob investigação presentes e aceites no decorrer da dissertação.

5.1 Principais Considerações Finais

Com a execução da presente dissertação sobre a auditoria a tecnologia no 5G no âmbito da Cibersegurança e dos SI, pensa-se ter sido possível criar uma base generalizada de conhecimento inicial, relativamente aos problemas que os auditores poderão vir a ter de enfrentar no decurso da persecução da sua atividade. Com esta reunião de informação através do levantamento de três temas de investigação, é entregue aos auditores uma visão global dos desafios com que se irão defrontar no exercício das suas funções.

O constante desenvolvimento de novas ameaças, o aumento dos ataques cibernéticos, o roubo de informação, dados privilegiados e privados e o crime de extorsão, vai exigir que as empresas estejam cada vez mais conscientes da importância da proteção dos seus dados e da sua informação, bem como, um acompanhamento e aconselhamento de uma pessoa e/ou entidade experiente, especializada e atenta a esta temática.

O 5G será um forte aliado da Cibersegurança e de uma cada vez mais apertada regulamentação de proteção de dados, quer seja na confidencialidade dos mesmos, quer seja na sua divulgação, sendo natural que existam preocupações acrescidas nas auditorias informáticas a realizar, uma vez que as redes móveis são áreas potencialmente difíceis de auditar.

Na Cibersegurança, a educação (preparação), a formação (aquisição de competências) e a capacitação (enfoque em problemas e questões fulcrais, onde é necessária perceção e adequação no *modus operandi*) funcionam como um complemento crucial para uma preparação mais adequada.

Foi por isso possível aferir ao longo dos capítulos desta dissertação que as tecnologias estão a evoluir cada vez mais rapidamente, o que interfere com as atividades das entidades e que por consequência afetam também o trabalho da auditoria.

Como referido no resumo e no capítulo da introdução, foi pretendido com a elaboração deste projeto de investigação, a interpretação, a desmistificação e o alerta para a adaptabilidade e para a preparação da área da auditoria para estes novos paradigmas. É importante que a ASI comece a criar políticas de conformidade que minimizem os riscos e potenciem a licitude da recolha dos dados, bem como, o seu tratamento e respetivo armazenamento, por forma a salvaguardar as entidades com a futura implementação do 5G.

Para a área da auditoria, todos os avanços tecnológicos não só têm melhorado o processo como têm criado alguns obstáculos e dificuldades para a atividade. A auditoria sendo uma área que necessita de estar em constante evolução e adaptação para com os novos paradigmas exigidos pelo mercado deverá abandonar definitivamente a função de entidade fiscalizadora e assumir uma função mais proactiva, de avaliação e de consultoria de forma a apoiar as entidades.

Em resposta ao tema principal de investigação, verificou-se que o sistema 5G é uma temática ainda muito recente e com a existência de inúmeras incógnitas para a comunidade em geral. Assim, a área do 5G e da auditoria ainda não carece de grande acoplagem não tendo sido possível através da presente dissertação apresentar qualquer tipo de conclusão relacionada com estas duas dimensões.

5.2 Limitações ao Estudo e Perspetivas Futuras

Todas as dissertações têm limitações e a presente não é exceção. Algumas delas, associadas ao método de investigação utilizado.

Uma das principais limitações para o estudo deste tema prendeu-se com o facto de ainda existirem muitas incógnitas no que se refere ao 5G. É sabido que à presente data o 5G começa a dar os primeiros passos no nosso país à semelhança de outros países onde o 5G já funciona, embora de forma muito precoce. Sucede que esses países já iniciaram a sua massificação.

Em Portugal um dos poucos sinais de que existe da chegada iminente do 5G, para além dos *Smartphones*, foi a transmissão holográfica ocorrida em 2019 pela TVI no Vodafone Paredes de Coura através da demonstração do potencial da rede 5G da Vodafone e o leilão que decorreu entre as operadoras nacionais para a atribuição de direitos de utilização de determinadas frequências associadas diretamente a esta nova rede móvel.

Assim, pelo facto de as entidades ainda estarem numa fase muito inicial da utilização deste tipo de tecnologia, torna-se difícil relacionar a atividade da auditoria com a utilização por parte das entidades do 5G.

Relativamente às perspetivas futuras, no decorrer do desenvolvimento desta dissertação foram tomadas várias decisões que pela sua importância deram características peculiares à dissertação, isto é, a dissertação poderia ter sido realizada segundo um diferente conjunto de decisões ou métodos de investigação e por esse facto o mesmo tema pode dar origem a novas oportunidades de estudo para futuras dissertações.

As sugestões a seguir apresentadas são meros guias de compreensão que podem vir a ser utilizadas para dar continuidade ao trabalho apresentado:

- Verificar como a implementação do 5G potenciou a exposição das empresas a novos riscos;
- Desenvolvimento de um método que proteja as empresas aquando da adoção desta nova tecnologia.

Como corolário, salvaguardam-se todos os trabalhos de auditoria já realizados por equipas multidisciplinares competentes no âmbito da segurança a SI, bem como, auditorias já realizadas à tecnologia 4G e anteriores.

Por questões de confidencialidade e ausência de respostas a quem faz estes trabalhos especializados, não foi possível relacionar outras evidências decerto conhecidas.

Apresenta-se também como sugestão, futuras linhas de investigação associadas à Cibersegurança, ao abrigo do protocolo existente entre o IPL e o CNCS.

Referências Bibliográficas

ADSL Fibra, Rede 5G em Portugal: será que estamos preparados para as mudanças? Disponível em: https://adslfibra.pt/servicos-gestoes/cobertura/5G

Almeida, B. (2005). *Auditoria e Sociedade - Diferenças de Expectativas*. Portugal: Editora Publisher Team, SA.

Alter, S. (1992). *Information Systems: A Management Perspective* (M. Reading, Ed.) Londres: Addison Wesley.

Amaral, L.A.M.d., PRAXIS: *Um referencial para o Planeamento de Sistemas de Informação*, Tese de Doutoramento, Universidade do Minho, 1994 (in portuguese).

ANACOM, *ANACOM publica guia com os factos, dados e desafios do 5G*. Disponível em: https://www.anacom.pt/render.jsp?contentId=1540981

ANACOM, *Redes Móveis e Saúde – Factos, Dados e Desafios*. Disponível em: https://fliphtml5.com/rchw/unvq

Andrade, António e Julião, Jorge (2019) – *Sistemas de Informação e Tecnológicos*, Porto: Universidade Católica Editora Porto

APD, *Tecnologia 5G: vantagens e desvantagens para as empresas*. Disponível em: https://www.apd.pt/tecnologia-5g-vantagens-e-desvantagens-para-as-empresas/

APDC, *Relatório sobre o risco de cibersegurança no 5G está concluído*. Disponível em: https://www.apdc.pt/noticias/atualidade-nacional/relatorio-sobre-o-risco-de-ciberseguranca-no-5g-esta-concluido

Arens, A. A., Randal, J. E., & Beasley, M. S. (2003). *Auditing and Assurance Services - An Integrated Approach (Ninth Edition)*. New Jersey: Prentice Hall.

Ashbaugh, H., & Warfield, T. D. (2003). *Audits as a corporate governance mechanism: Evidence from the German market*. *Journal of International Accounting Research.*

ATEC, *A nova tecnologia 5G*. Disponível em: https://www.atec.pt/artigos-tecnicos/a-nova-tecnologia-5G-esta-para-breve.html

Aziz, Osman Abdul (2019). *Auditoria aos Sistemas de Informação com base no Control Objectives for Information and related Technology (COBIT).* Disponível em: https://repositorio.ipl.pt/bitstream/10400.21/12170/1/Definitiva_Dissertacao_Audi

toria_SI_COBIT_20170188_Osman_Aziz_2019_.pdf

Baharuddin, N. H., *et al*. (2019). *Global Perspectives and Insights – 5G and the Fourth Industrial Revolution Part II*. Disponível em https://docs.ifaci.com/wp-content/uploads/2019/07/5G-and-the-Fourth-Industrial-Revolution-Part-2.pdf

Baptista da Costa, Carlos - *Auditoria Financeira – Teoria e Prática. 9a edição*. Lisboa: Rei dos Livros, 2010. ISBN 978-989-8305-11-4.7084-1

Baptista, C. S., e Sousa, M. J. (2011) – *Como Fazer Investigação, Dissertações, Tese e Relatórios – Segundo Bolonha*. Lisboa: Pactor. ISBN 978-989-69300-11

Bedoya, L. D., *et al*. (2016). *Global Perspectives and Insights – Elevando o Impacto Estratégico da Auditoria Interna.* Disponível em: https://global.theiia.org/translations/PublicDocuments/GPI-Elevating-Internal-Audits-Strategic-Impact-Portuguese,pdf

Bell, T. B., & Tabor, R. H. (1991). *Empirical analysis of audit uncertainty qualifications. Journal of Accounting Research*.

Buckingham, R. A., Hirschheim, R. A., Land, F. F., & Tully, C. J. (Eds). (1987). *Information systems education: Recommendations and implementation.* Cambridge: Cambridge University Press.

CISCO, *The Zettabyte Era Officially Begins (How Much is That?).* Disponível em: https://blogs.cisco.com/sp/the-zettabyte-era-officially-begins-how-much-is-that

CNCS. Centro Nacional de Cibersegurança Portugal, *Sobre Nós*. Disponível em: https://www.cncs.gov.pt/sobre-nos

CNET, *US finds Huawei has backdoor acess to mobile networks globally, report says*. Disponível em: https://www.cnet.com/news/us-finds-huawei-has-backdoor-access-to-mobile-networks-globally-report-says

COSO - Committee of Sponsoring Organizations of the Treadway Commission. (2013). Internal Control - Integrated Framework: Executive Summary. Durham: COSO.

Costa, C. B. (2007). *Auditoria Financeira (8a Ed).* Lisboa: Editora Rei dos Livros.

Costa, C. B. (2014). *Auditoria Financeira, Teoria e Prática. (10.ª Ed.).* Lisboa: Rei dos Livros.

Davenport, T. & Prusak, L. (1998). *Conhecimento Empresarial*. Rio de Janeiro: Campus.

Diário de Notícias, *A conspiração que liga Covid e rede 5G*. Disponível em: https://www.dn.pt/dinheiro/a-conspiracao-que-liga-covid-e-rede-5G-12059916.html

Deloitte, *Impact of 5G on Portugal* (2019). Disponível em: https://www2.deloitte.com/content/dam/Deloitte/pt/Documents/Hottopics/5G-Impact-on-Portugal.pdf

Deloitte, *Quem vai beneficiar com o 5G*. Disponível em: https://www2.deloitte.com/pt/pt/pages/technology-media-and-telecommunications/articles/quem-vai-beneficiar-com-o-5G.html

Deloitte, *Securing Telcos' 5G adoption journey*. Disponível em: https://www2.deloitte.com/pt/pt/pages/technology-media-and-telecommunications/articles/Securing-Telcos-5G-adoption-journey.html

Dinheiro Vivo, *O futuro da cibersegurança com o 5G*. Disponível em: https://www.dinheirovivo.pt/opiniao/o-futuro-da-ciberseguranca-com-o-5g-14249424.html

EDPB, *e-Privacy Regulation*. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/topic/e-privacy-regulation_pt

ENISA (2019) ENISA Threat Landscape Report 2018, ENISA-European Union Agency for Cybersecurity.

ESET Portugal Blog, UE alerta para riscos de cibersegurança associados ao 5G. Disponível em: https://blog.eset.pt/2019/10/ue-alerta-para-riscos-de-ciberseguranca-associados-ao-5g/

Fox Business, *Nokia to cut jobs in focus on 5G*. Disponível em: https://www.foxbusiness.com/markets/nokia-to-cut-jobs-in-focus-on-5G

Grenier, R. & Metes, G. (1992). *Enterprise Networking.* Boston: Digital Press.

Identity Force – A Sontiq Brand, *2017 Data Breaches | The Year of Equifax.* Disponível em: https://www.identityforce.com/blog/2017-data-breaches

IIA - The Institute of Internal Auditors. *The Institute of Internal Auditors – Definition of Internal Auditing*. [Consult. 9 junho 2019]. Disponível em: https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Definition-of Internal-Auditing.aspx

ISACA – Cobit 4.1 Português. 2007. Disponível em: http://www.isaca.org/Knowledge-Center/cobit/Documents/cobit41-portuguese.pdf

ISO 9001:2015 – Sistema de gestão de qualidade. Disponível em: https://www.iso.org/standard/62085.html

ISO 27001:2013 – Sistema de gestão de segurança da informação. Disponível em: https://www.iso.org/standard/54534.html

Diário da República, Lei n.º 46/2018, n.º 155/2018, Série I de 2018-08-13. [Consult. 11 novembro 2019]. Disponível em: https://dre.pt/application/conteudo/116029384

Jornal de Noticias, *Tudo o que precisa de saber sobre a rede 5G*. Disponível em: https://www.jn.pt/inovacao/tudo-o-que-precisa-de-saber-sobre-a-rede-5G-10718758.html

Kaplan, R.S. e Norton, D.P. (1996), "The Balanced Scorecard: Translating Strategy into Action", Boston: HBS.

Ketele, Jean-Marie De & Roegiers, Xavier (1999). *Metodologia da recolha de dados*. Lisboa: Instituto Piaget.

KPMG, *A promessa do 5G*. Disponível em: https://home.kpmg/br/pt/home/insights/2020/11/promessa-investidor-5g.html

Le Moigne (1978). *La Theorie du système d'information organisationnel*. Informatique et Gestion, n. º 101, 102, 103 e 104.

Lucas, H. (1987). *Information Systems, Concepts for Management.* New York: McGraw-Hill.

Martins, Ivan (2013). *Auditoria dos sistemas de informação das instituições financeiras.* Lisboa: ISCAL.

Máximo Consultoria, *Quais os Benefícios do 5G para o mundo empresarial*. Disponível em: https://maximoconsultoria.com/beneficios-5g-para-mundo-empresarial/

MDS *Brokerslink*, *Aumenta a dimensão do risco cibernético*. Disponível em: https://www.mdsgroup.pt/pt/noticias/aumenta-a-dimensao-do-risco-cibernetico

Morais, G., e Martins, I. (2007). Auditoria Interna: função e processo (3.a ed.). Áreas Editora.

Nabais, António C. Maia (1993) *"Museus de Região"*. In Rocha-Trindade, M. Beatriz (coord.) Iniciação à Museologia. Lisboa: Universidade Aberta.

NIST (2013) NIST IR 7298 Revision 2, Glossary of Key Information Security Terms, National Institute of Standards and Technology.

NOS, *5G*. Disponível em: https://www.nos.pt/particulares/5G/Pages/5G.aspx

O'Brien, J. A. (1990). *Management Information Systems – A managerial end user perspective.* Indiana: Irwin.

Observador, *Prepare-se para o futuro com o 5G*. Disponível em: https://observador.pt/explicadores/prepare-se-para-o-futuro-com-o-5G

Oliveira, A. de (2009). *Informação e Sistemas de Informação*. Lisboa: Refer Telecom.

Ortega y Gasset, José. *El hombre y la gente*. Madrid: Revista de Occidente, 2010.

Parlamento Europeu e do Conselho. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho publicado em 27 de abril de 2016. *Regulamento Geral de Proteção de Dados*. [Consult. 20 novembro 2019]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679

PLMJ, *Cibersegurança deve fazer parte do ADN das empresas.* Disponível em: https://www.plmj.com/pt/sobre-nos/noticias-plmj/noticias/Ciberseguranca-deve-fazer-parte-do-ADN-das-empresas/19377/

Portal 5G, S*egurança*. Disponível em: https://portal5g.pt/temas/seguranca/

Pplware, *Tecnologias 1G, 2G, 2.5G, 3G e 4G – Sabe a diferença? Disponível em:* https://pplware.sapo.pt/tutoriais/networking/tecnologias-1g-2g-2-5-g-3g-e-4G-sabe-a-diferena

Procuradoria-Geral Distrital de Lisboa. Lei n.º 166/98 do Ministério Público publicado em 17 de junho de 1998. *Sistema de Controlo Interno da Administração Financeira do Estado (SCI)*. Disponível em:

http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1625&tabela=leis

Procuradoria-Geral Distrital de Lisboa. Lei n.º 109/2009 do Ministério Público publicado em 15 de setembro de 2009. *Lei do Cibercrime*. Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_estrutura.php?tabela=leis&artigo_id=&nid=1137&nversao=&tabela=leis&so_miolo=

Procuradoria-Geral Distrital de Lisboa. Lei n.º 46/2018 do Ministério Público publicado em 13 de agosto de 2018. *Regime Jurídico da Segurança do Ciberespaço*. Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?tabela=leis&artigo_id=&nid=2930&nversao=&tabela=leis&so_miolo=S

Prodanov, C., & Freitas, E. (2013). *Metodologia do trabalho científico. Métodos e técnicas da pesquisa e do trabalho acadêmico.* Novo Hamburgo: Universidade FEEVALE.

Proteção de dados. Disponível em: https://protecao-dados.pt

PwC, Conferência "*Cibersegurança – Os desafios da Tecnologia Operacional (OT)*". Disponível em: https://www.pwc.pt/pt/eventos/2020/ciberseguranca.html

PwC, *The Global Economic Impact of 5G*. Disponível em: https://www.pwc.pt/pt/temas-actuais/the-global-economic-impact-of-5g.html

Resolução do Conselho de Ministros n.º 92/2019 n.º 108/2019, Série I de 2019-06-05. [Consult. 11 novembro 2019]. Disponível em: https://dre.pt/application/conteudo/122498962

Sapo, *Operadores dão os primeiros passos no 4G*. Disponível em: https://tek.sapo.pt/noticias/telecomunicacoes/artigos/operadores-dao-os-primeiros-passos-no-4G

Sapo, *5G é peça essencial na transformação digital*. Disponível em: https://visao.sapo.pt/exameinformatica/noticias-ei/brand-studio/2021-10-28-5g-e-peca-essencial-na-transformacao-digital/

Sapo, *5G: E depois do "big bang"?* Disponível em: https://visao.sapo.pt/exame/2021-04-01-5g-e-depois-do-big-bang/

Sawyer, Lawrence B.; [et al.] – Sawyers' Internal Auditing – *The practice of Modern Internal Auditing*. EUA: The Institute of Internal Auditors, 2005. ISBN 0-89413- 509-0.

Security Magazine, *Garantir a visão da EU em 5G: Certificação de Cibersegurança*. Disponível em: https://www.securitymagazine.pt/2021/05/17/garantir-a-visao-da-ue-em-5g-certificacao-de-ciberseguranca/

Sicomtesting, *Da primeira para a quinta geração, o passado e o futuro de padrões de telecomunicações.* Disponível em: https://www.sicomtesting.com/pt/blog/dal-1g-al-5G-il-passato-e-il-futuro-degli-standard-gsm-umts-hspa-ed-lte/

Taborda, D. (2015). *Auditoria - Revisão Legal das Contas e Outras Funções do Revisor Oficial de Contas (2a Edição).* Lisboa: Edições Sílabo.

Teixeira, M. (2006), *O contributo da Auditoria Interna para uma Gestão eficaz*, Dissertação de Mestrado em Contabilidade e Auditoria.

TrendMicro, *Segurança 5G para empresas*. Disponível em: https://www.trendmicro.com/pt_br/business/solutions/iot/enterprise-5g-iot.html

TVI 24, *Afinal que evidências há que o 5G é um perigo para a nossa saúde?* Disponível em: https://tvi24.iol.pt/tecnologia/economia/afinal-que-evidencias-ha-de-que-o-5G-e-um-perigo-para-a-nossa-saude

T-Mobile For Business, *What's your roadmap to enterprise 5G adoption?* Disponível em: https://www.t-mobile.com/business/trends-and-insights?src=spr&rdpage=https%3A%2F%2Fbusiness.sprint.com%2Fblog%2F5G-business-transformation%2F&limit=6&page=1#content-hub-articles

Valor Magazine, *Operational technology: a nova fronteira da cibersegurança*. Disponível em: https://www.valormagazine.pt/operational-technology-a-nova-fronteira-da-ciberseguranca

Vodafone, *Vodafone Portugal já tem 5G para testes em Lisboa*. Disponível em: https://www.vodafone.pt/press-releases/2019/3/vodafone-portugal-ja-tem-5G-para-testes-em-lisboa.html

Wired, *The Worst Cybersecurity Breaches of 2018 So Far*. Disponível em: https://www.wired.com/story/2018-worst-hacks-so-far.