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

RISCOS CIBERNÉTICOS NAS INSTITUIÇÕES FINANCEIRAS

AVALIAÇÃO DAS ESTRATÉGIAS DE MITIGAÇÃO DE RISCOS CIBERNÉTICOS NA CAIXA ECONÓMICA DE CABO VERDE

Ilídio Cardoso Mendes

Lisboa, Fevereiro de 2025

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

RISCOS CIBERNÉTICOS NAS INSTITUIÇÕES FINANCEIRAS

AVALIAÇÃO DAS ESTRATÉGIAS DE MITIGAÇÃO DOS RISCOS CIBERNÉTICOS NA CAIXA ECONÓMICA DE CABO VERDE

Ilídio Cardoso Mendes

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Lisboa para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Gestão das Instituições Financeiras, realizada sob a orientação científica do Professor Doutor Raúl Daniel Navas, Professor Adjunto no ISCAL/Instituto Politécnico de Lisboa, Economista.

Constituição do Júri:
Presidente: Doutora Ana Maria Sotomayor
Arguente: Doutora Denise Miriam Mendes Torrão
Vogal: Doutor Raúl Daniel Navas

Lisboa, Fevereiro de 2025

Dissertação elaborada ao abrigo do projeto
IPL/IDI&CA2024/CRYPTORISK_ISCAL.

DEDICATÓRIA

Aos meus pais, os mais
importantes mestres/professores
de um filho.

In memoriam of my partner,
Nicky (2024.07.30)

EPÍGRAFE

"Tem 2 tipo di sonhu: tem kel sonhu q bu ta sunha ta durmi, geralmente di cuzas passado e desejos q ka realiza. E tem sunha cordadu, sunha ku um cuza futuro q bu cre realiza."

~ José Maria Neves,
Presidente da República de Cabo Verde

AGRADECIMENTOS

Primeiramente, agradecer aos meus pais, pelo apoio e por reunir condições mais do que necessárias para a realização do mestrado num país estrangeiro.

Agradeço a minha família presente em Portugal, por me fazerem sentir em casa mesmo estando longe de casa.

Ao meu orientador, pela disponibilidade, sugestões e linhas de orientação.

À Caixa Económica de Cabo Verde pela disponibilidade em colaborar no estudo, um excelente exemplo para outras entidades no incentivo à investigação.

A todos os professores, principalmente pela ajuda na fase inicial do mestrado, iniciado com 2 meses de atraso.

Por último, aos amigos por todo o apoio necessário para seguir cada jornada.

RESUMO

Num mundo cada vez mais globalizado e tecnológico, as instituições financeiras oferecem serviços e produtos cada vez mais vantajosos e de fácil acesso para os clientes, fruto das transformações digitais a que todos os serviços estão sujeitos, impulsionado ainda mais pela pandemia da Covid-19. Contudo, as tecnologias não trazem somente benefícios aos clientes e às instituições: aliado à transformação digital, as instituições financeiras estão também sujeitas a um conjunto de ameaças e riscos digitais, isto é, aos ataques cibernéticos. Com isso, destaca-se o importante papel da cibersegurança das instituições financeiras na salvaguarda dos dados e das informações, tanto da instituição como dos clientes. Com este trabalho pretende-se de uma forma geral analisar e conhecer conceitos relacionados com os riscos cibernéticos e segurança cibernética, procurando associar estes conceitos no contexto das instituições financeiras e suas consequências para estas instituições e para a própria estabilidade económica. Numa vertente mais prática do trabalho, pretende-se realizar um estudo sobre a avaliação das estratégias de mitigação de riscos cibernéticos na Caixa Económica de Cabo Verde, uma das maiores instituições financeiras do país.

Palavras-chave: Instituições financeiras; ataques cibernéticos; riscos cibernéticos; cibersegurança; ISO 27001; CECV.

ABSTRACT

In an increasingly globalized and technological world, financial institutions offer advantageous and accessible services and products to customers as a result of the digital transformations to which all services are subject, accelerated by the Covid-19 pandemic. However, technology does not only bring benefits to customers and institutions: along with digital transformation, but financial institutions are also exposed to a set of digital threats and risks, namely cyberattacks. This highlights the crucial role of cybersecurity in financial institutions in safeguarding data and information, both institution and its customers. This work aims, in a general sense, to analyze and to understand concepts related to cyber risks and cybersecurity, seeking to link these concepts to the context of financial institutions and their consequences for these institutions and economic stability. On a practical level, the work aims to conduct a study on the evaluation of strategies for mitigating cyber risks at Caixa Económica de Cabo Verde, one of the largest financial institutions in the country.

Key Words: Financial institutions; cyber-attacks; cyber risks; cybersecurity; ISO 27001; CECV.

ÍNDICE

ÍNDICE DE QUADROS

ÍNDICE DE TABELAS

ÍNDICE DE FIGURA

LISTA DE ABREVIATURAS/SÍMBOLOS

CECV – Caixa Económica de Cabo Verde

CERT – *Computer Emergency Response Team* (Equipa de Resposta a Emergências Informáticos)

CIRT – *Computer Incident Response Team* (Equipa de Resposta a Incidentes Informáticos)

CSIRT – *Computer Security Incident Response Team* (Equipa de Resposta a Incidentes de Segurança Informática)

CNCS – Centro Nacional de Cibersegurança

DDoS - *Distributed Denial of Services (*Negação de Serviços)

E1 – Entrevista 1 (Departamento de Comunicação, Informática e Segurança)

E2 – Entrevista 2 (Administradores de Rede)

EIOPA – *European Insurance and Occupational Pensions Authority* (Autoridade Europeia de Seguros e Pensões Ocupacionais)

ENC – Estratégia Nacional para a Cibersegurança

ENISA – *European Network and Information Security Agency* (Agência Europeia para a Segurança das Redes e da Informação)

I1 – Indivíduo 1 (Colaborador da área de Comunicação, Informática e Segurança)

I2 – Indivíduo 2 (Administrador de Rede)

I3 – Indivíduo 3 (Administrador de Rede)

IA – Inteligência Artificial

ISO - *International Organization for Standardization* (Organização Internacional de Normalização)

ITU - *International Telecommunication Union* (União Internacional de Telecomunicações)

NIST – *National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologias)

NNCS – Núcleo Nacional de Cibersegurança

Q1 – Questionário destinado aos colaboradores

Q2 – Questionário destinado a clientes

SPSS – *Statistical Package for the Social Sciences* (Pacote Estatístico para as Ciências Sociais)

1. INTRODUÇÃO

Num mundo de constantes evoluções e transformações, marcada por eras de profundas revoluções, encontramo-nos hoje num mundo marcado essencialmente pela transformação digital. As tecnologias estão presentes em praticamente todos os momentos do nosso quotidiano, desde tarefas mais complexas às mais simples, graças aos benefícios proporcionados. Tal como Silva e Ferrari (2023) destacam, as tecnologias de informação e comunicação são atualmente bens essenciais na sociedade, sendo a Internet uma peça fulcral na interconexão entre os sistemas de informação. O mesmo acontece no mundo empresarial. Organizações públicas e privadas dependem de tecnologias de informação e sistemas de informação para que consigam cumprir com sucesso as suas missões e funções (*National Institute of Standards and Technology* - NIST, 2012). A digitalização tem revolucionado empresas de todos os setores, não sendo exceção o setor financeiro. A necessidade das instituições financeiras em adotar novos métodos, técnicas e ferramentas para melhor atingirem os seus objetivos e satisfazerem as necessidades da sociedade é uma constante, sendo a transformação digital uma das principais evoluções verificadas nos últimos tempos. A digitalização das operações financeiras tem permitido às instituições financeiras modernizarem os seus serviços, melhorarem a experiência do cliente e expandirem a sua competitividade no mercado global.

De entre as várias vantagens trazidas pelo processo de digitalização das instituições financeiras, nomeadamente facilidades no levantamento de montantes, transferências nacionais e internacionais e o pagamento (Elliot & Jenkinson, 2020), encontra-se aliado um conjunto de ameaças, nomeadamente riscos cibernéticos. De acordo com Alegria, Montoya, Loayza e Armas-Aguirre (2022), o processo de transformação digital do setor financeiro potencia o aparecimento de ameaças cibernéticas, sendo este setor dos mais afetados dentro das várias indústrias. É neste sentido, e dado ao papel fulcral das instituições financeiras na economia e nas sociedades, que o termo cibersegurança ou segurança cibernética tem ganho importante destaque na estabilidade das instituições financeiras e do próprio sistema financeiro, sendo considerado pelo Instituto Americano de Contabilistas Públicos Certificados (2018 cit in Masoud e Al-Utaibi, 2022) como uma das principais preocupações da administração de qualquer empresa, grande ou pequena, privada ou pública.

Com isso, a presente dissertação tem por título "Riscos Cibernéticos nas Instituições Financeiras", um tema bastante pertinente nos dias de hoje, motivado pela constante evolução digital e pela importância das instituições financeiras. Ao longo da dissertação pretende-se realizar um estudo cujo objetivo consiste na avaliação das estratégias de mitigação de riscos cibernéticos na Caixa Económica de Cabo Verde (CECV), um dos maiores bancos e instituições financeiras do país.

Para realização do estudo, primeiramente fez-se uma revisão de literatura por forma a familiarizar com o tema em estudo, uma vez que os conhecimentos sobre a matéria são limitados. A investigação será um estudo de caso, uma vez que se pretende analisar o caso específico da CECV.

Assim, a dissertação encontra-se estruturada em 5 capítulos sendo o primeiro a presente Introdução.

O segundo capítulo consiste numa Revisão de Literatura com foco nos conceitos essenciais relacionados com os riscos cibernéticos, nos tipos de ataques cibernéticos e na cibersegurança. Também, abordou-se o contexto de cibersegurança da entidade alvo do estudo.

No terceiro capítulo, foi enunciado a metodologia utilizada no estudo. Definiu-se o método de investigação, os objetivos de investigação, as técnicas utilizadas para recolha de dados, e os métodos de seleção e análise dos mesmos.

O quarto capítulo destinou-se ao estudo de caso propriamente dito, iniciando por uma breve apresentação da empresa em estudo e seguido pela aplicação das técnicas mencionadas na metodologia.

Durante o quinto e último capítulo, expôs-se as principais conclusões quanto ao estudo realizado. Foram enunciadas as limitações verificadas durante o estudo e foram sugeridas algumas dicas para futuras investigações na área. Finalizou-se com breves considerações finais sobre a elaboração da presente dissertação.

2. REVISÃO DA LITERATURA

Ao longo deste capítulo de Revisão de Literatura será feito um enquadramento com o tema em termos de conceitos relacionados, por forma adquirir conhecimentos e familiarizar com o tema para melhor dar seguimento com o estudo. Também, compreender a importância das instituições financeiras para a estabilidade financeira, os impactos da globalização, da digitalização e da pandemia, bem como os ataques cibernéticos mais frequentes. Será abordado a temática da cibersegurança, com destaque para o normativo ISO 27001, finalizando com uma análise do contexto cibernético nacional de Cabo Verde, localização geográfica da empresa a ser estudada.

2.1. CONCEITOS

Num mundo atual cada vez mais marcado pelas tecnologias, o processo da digitalização é já uma realidade em quase todos os serviços em que nos expomos no nosso dia-a-dia, desde lazer até aos mais prioritários, como a saúde. Um dos acontecimentos marcantes da era da digitalização é, sem dúvida, o aparecimento da internet que, segundo Camilo (2021), foi ativada pela primeira vez em 1969 pela ARPANET, desenvolvendo significativamente áreas da ciência relacionadas com a tecnologia, informática, computação e o digital.

O setor financeiro tem sido alvo de constantes mudanças, inovações e evoluções, fruto de transformações em relação a sistemas e tecnologias de informação, isto é, a digitalização de processos, produtos e serviços oferecidos, agregando um conjunto de valores e vantagens tais como rapidez e facilidade. Elliot e Jenkinson (2020) destacam o papel que a pandemia do covid-19 teve na aceleração do processo de transformação digital das instituições financeiras, sendo que para estes autores a pandemia veio ilustrar o importante papel da conexão digital para os seres humanos atualmente.

Para Dudin *et al.* (2021, *cit in* Ferreira, Marton & Perez, 2022), o aparecimento da pandemia fez com que os serviços virtuais oferecidos pelos bancos (trabalho remoto e *mobile banking*, por exemplo) se tornassem mais vulneráveis e expostos a um conjunto de riscos cibernéticos, isto é, **ataques cibernéticos**. Segundo o Instituto Nacional de Padrões e Tecnologias (NIST, 2012), um ciberataque pode ser definido como um ataque ao ciberespaço de uma empresa, cujo objetivo pode ser perturbar, desabilitar, destruir

ou controlar maliciosamente o ambiente/infraestrutura virtual da empresa; ou destruindo a integridade de dados ou roubar informações.

Neste contexto, torna-se importante compreender o conceito de **ciberespaço**, que pode ser definido como "*the notional environment in which electronic communication occurs*" (Kuehl, 2009, pp.5 cit in Balão, 2014, pp.210), isto é, o mundo virtual de uma instituição financeira, não só interna como externa. Para o NIST (2012), o ciberespaço trata-se de um domínio mais abrangente, a nível global, dentro do ambiente informacional, que por sua vez compreende redes interdependentes de infraestruturas de sistemas de informação, incluindo a Internet, redes de telecomunicações e sistemas informáticos.

Com isso, a proteção do espaço virtual das instituições financeiras acaba por ser de extrema importância tendo em conta o fluxo de informações e dados privados não só da empresa, mas também dos clientes, sendo que, de acordo com Alegria *et al.* (2022), a segurança dos dados dos clientes é considerada um ativo crítico na conquista da confiança dos clientes na disponibilização das suas informações. Adelmann *et al.* (2020) acrescenta ainda que, devido à grande dependência dos dados por parte dos serviços financeiros, a vulnerabilidade e a complexidade da cibersegurança acaba por ser ainda maior. O conceito de **cibersegurança** (ou segurança cibernética) surge em 1960 (Ware, 1967 *cit in* Ferreira *et al.*, 2022, pp. 176) e para o NIST (2012, pp. B-1) pode ser simplesmente compreendida como *"*a habilidade de proteger ou defender o uso do ciberespaço de ataques cibernéticos". A União Internacional de Telecomunicações (n.d., *cit in* Ferreira *et al.*, 2022, pp.176), por sua vez, dá uma definição mais prolongada, sendo que para estes a cibersegurança é compreendida como sendo

> a coleta de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, abordagens de gerenciamento de riscos, ações, treinamento, melhores práticas, garantias e tecnologias que possam ser usadas para proteger o ambiente cibernético, a organização e os ativos do usuário. (União Internacional de Telecomunicações, n.d., *cit in* Ferreira *et al.*, 2022, pp.176)

A nível físico e estrutural, as instituições financeiras estão expostas a várias ameaças e podem ser danificadas por negligência, por atos deliberados, ou por fenómenos naturais. Simultaneamente e devido à constante evolução digital, as instituições

financeiras estão expostas a um conjunto de riscos aliados ao mundo digital, isto é, aos **riscos cibernéticos**. De acordo com o Banco Mundial (2018, *cit in* Masoud & Al-Utaibi, 2022, 133), o setor financeiro foi a indústria que mais sofreu ataques no ano de 2016, comprovando a ideia de Adelmann *et al.* (2020) que afirma que os serviços financeiros são a indústria que mais sofre ataques cibernéticos tendo em conta a sua vulnerabilidade e atratividade. Por estes e outros motivos, cada vez mais aumenta o número de **cibercriminosos**, definido pelo Centro Nacional de Cibersegurança de Portugal (CNCS, 2023) como indivíduos ou grupos que atuam de forma maliciosa no ciberespaço com a única finalidade de obter ganhos económicos. No âmbito deste trabalho, refere-se a cibercriminosos como os agentes individuais ou coletivos que praticam crimes cibernéticos com motivos diversos, e não exclusivamente ganhos financeiros. Não obstante obter ganhos financeiros ser o principal motivo da prática de cibercrimes, a Agência para a Segurança das Redes e da Informação através do mais recente relatório *Thread Landscape* (ENISA, 2023) acrescenta ainda a espionagem, a disrupção, a destruição e ideologias como outros fatores que podem motivar os cibercriminosos, surgindo outros termos relacionados. ***Crackers***, por exemplo, são aqueles que praticam cibercrimes com o objetivo de criar disrupção ou interrupção no sistema das vítimas e ganhar reputação (Bruijne *et al. cit in* CNCS, 2023). ***Hacktivistas*** são cibercriminosos, normalmente com poucos recursos, cujo objetivo é impor uma determinada afirmação, ideologia ou mudança social, tendo como vítimas preferidas grupos políticos, como descreve a ENISA (2023).

2.2. ESTABILIDADE FINANCEIRA E A IMPORTÂNCIA DAS INSTITUIÇÕES FINANCEIRAS

A estabilidade financeira é um pilar essencial para o crescimento económico sustentável, e as instituições financeiras desempenham um papel crucial nesse processo. Gulyás e Kiss (2023) referem a esse importante papel das instituições financeiras na economia uma vez que asseguram a liquidez, a oferta monetária na economia, possibilitam a concessão de empréstimos, as poupanças e os depósitos, além de garantirem a operacionalização dos sistemas de pagamentos.

Atualmente as instituições financeiras estão sujeitas a um conjunto de riscos, nomeadamente riscos derivados de ataques cibernéticos. Tendo em conta a importância

das instituições para a estabilidade do sistema financeiro, considerado a "espinha dorsal" da economia, pode-se afirmar que um ciberataque a uma instituição financeira se traduz num ataque à economia, podendo causar graves consequências (Gulyás & Kiss, 2023). Com isso, de acordo com Pollmeier, Bongiovanni e Slapnicar (2023), cada vez mais é a preocupação com os impactos causados por possíveis ataques cibernéticos na estabilidade financeira, podendo ser um deles a perda de confiança no sistema financeiro e na economia global, como acrescentam Gulyás e Kiss (2023). Para estes autores, a manipulação da economia global passou mesmo a ser a principal motivação dos cibercriminosos, ao invés do roubo de dados pessoais e de ganhos financeiros.

Huang e Xu (2000) constataram o facto curioso de que crises financeiras são frequentemente acompanhadas por problemas em instituições financeiras. De facto, crises financeiras recentes, como a crise do *subprime* em 2007-2008, tiveram sua origem e ligação com problemas em instituições financeiras. Na opinião de Gulyás e Kiss (2023), devido à grande interconetividade do setor financeiro, explicada pela ligação entre as instituições financeiras através das relações interbancárias e utilização de dados de fontes comuns (Adelman *et al.*, 2020) e impulsionada pela globalização, o sistema financeiro global apresenta um elevado risco sistémico. Isto significa que mesmo um pequeno ataque a uma instituição poderá ter consequências graves para todo o sistema financeiro. Adaptando esta lógica a ataques cibernéticos resulta no conceito de risco cibernético sistêmico que consiste no risco de um único incidente cibernético numa infraestrutura crítica do sistema causar impactos significantes para outros componentes do sistema, impactando por exemplo todo o sistema económico, de acordo com o World Economic Forum (2016). Portanto, tendo em conta as caraterísticas do setor financeiro, nomeadamente a interconetividade e a globalização, fazem com que o setor tenha elevado risco sistémico e efeito contágio entre os componentes, sendo que, segundo Huang e Xu (2000), as economias menos desenvolvidas resultam em menos riscos de contágio devido a homogeneidade e menos incertezas no mercado.

Com isso, devido ao importante papel e as funções desempenhadas pelas instituições financeiras na economia global, o setor financeiro merece atenção especial no que diz respeito às ameaças, nomeadamente as ameaças cibernéticas Gulyás e Kiss (2023).

2.3. EVOLUÇÃO E TIPOLOGIA DOS ATAQUES CIBERNÉTICOS

2.3.1. Globalização, Digitalização e Covid-19

Da mesma forma que as instituições, financeiras e não só, evoluíram e adaptaram as suas atividades de acordo com o aparecimento de novas tecnologias de informação e da era da transformação digital, os crimes cibernéticos também sofreram evoluções, ganhando sempre novas técnicas por forma a contornarem as barreiras criadas pelas instituições. Cada vez mais os ataques cibernéticos são mais sofisticados e evoluídos, procurando sempre acompanhar a evolução e o desenvolvimento de novas tecnologias, fazendo com que as instituições travem uma luta quase que constante contra o cibercrime por fim a mitigarem e eliminarem possíveis riscos cibernéticos.

Sem dúvida que o processo de transformação digital das instituições financeiras foi acelerado e impulsionado pelo aparecimento da pandemia Covid-19 em 2019, cujos efeitos tiveram maior dimensão a partir de 2020 (CNCS, 2021). Uma das principais medidas adotadas pelas instituições financeiras por forma a adaptarem-se às restrições impostas pelos organismos de saúde pública foi o confinamento e, por consequência, o trabalho remoto, o que de acordo com o Diretor Adjunto da FBI, Paul Abbate, *cit in* Gulyás e Kiss (2023) representou uma grande janela de oportunidades para os cibercriminosos, devido a grande dependência das tecnologias por parte das instituições. Partilhando das palavras de Gulyás e Kiss (2023), Frost e Shapiro (2022, *cit in* Pollmeier *et al., 2023*) também afirmam que a mudança acelerada para processos, produtos e serviços digitais por parte das instituições financeiras fez com que houvesse um aumento e intensificação de ataques cibernéticos às instituições, ao pessoal e aos próprios clientes. De acordo com Kellerman e Murphy (2020), através do estudo intitulado *Modern Bank Heist* 3.0 realizado em conjunto com 25 responsáveis pela segurança de instituições financeiras, houve um aumento de 238% no que diz respeito a ataques cibernéticos às instituições financeiras durante o aparecimento da pandemia, sendo que os ataques foram cada vez mais frequentes, sofisticados e destrutivos. Com números bastante similares, a FBI comunicou um aumento de 300% de crimes cibernéticos, tendo como consequência custos globais que atingiram 6 triliões de doláres em 2021 (Cybint, 2020 *cit in* Masoud & Al-Utaibi, 2022). Devido a esse número

cada vez mais crescente de ataques cibernéticos, a CNCS (2021) afirma que desde a covid-19 a cibersegurança passou a ser uma preocupação para salvaguardar a economia.

As falhas humanas têm sido referenciadas como uma das principais "brechas" aproveitadas pelos cibercriminosos, sendo de referir que de acordo com um relatório publicado pela Verizon, cerca de 44% dos ataques sofridos por instituições financeiras tiveram como origem falhas humanas, sendo que a maioria destes foram erros acidentais cometidos por funcionários internos destas instituições (*Verizon Data Breach Investigations Report*, 2021 *cit in* Gulyás & Kiss, 2023). O FBI destacou o erro humano como a principal causa dos crimes cibernéticos (Cybint, 2020 *cit in* Masoud & Al-Utaibi, 2022).

2.3.2. Principais ataques cibernéticos

A ENISA (2023), através do mais recente *Thread Landscape*, enumera como principais ameaças e ataques cibernéticos os seguintes:

- *Ransomware*
- *Malware*
- Engenharia Social (*Phishing* e *Smishing*)
- Ameaças contra dados
- Ameaças contra disponibilidade: *Denial of Service* e *Internet Threads*
- Manipulação e Interferência de Informações
- Ataques à cadeia de abastecimento

2.3.2.1. RANSOMWARE

Considerada pela ENISA (2023) como o ataque cibernético mais frequente, os ataques *ransomware* são definidos pelos mesmos como sendo *"a type of attack where thread actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability"* (pp.52). Na visão do NIST um ataque *ransomware* pode ser executado através de um *malware* através do qual o atacante consegue o controlo de dispositivos e dados de uma organização, bloqueando a possibilidade de esta poder aceder-lhes, e pede um resgate para que a organização recupere o controlo dos dispositivos e dados, sendo que em alguns casos é exigido o pagamento de quantias

adicionais para evitar a divulgação de informações confidenciais da organização (*cit in* ENISA, 2023). Assim, as características fundamentais desse tipo de ataque incluem os atacantes assumindo o controlo de dispositivos e dados (*assets),* e exigindo um pagamento para que a organização recupere o controle, conhecido como resgate (*ransom*), isto é uma chantagem (*blackmail)*. Com isso, considera-se os ganhos financeiros o principal motivo dos ataques *Ransomware*.

Gulyás e Kiss (2023) por sua vez referem aos ataques *ransomware* como o terceiro ataque mais comum nas instituições financeiras atrás do *phishing* e da engenharia social, sendo que estes autores destacam a pouca consciencialização por parte das instituições para com a cibersegurança, pois consideram que os cibercriminosos de ataques *ransomware* ainda utilizam *modus operandis* antigos, sobretudo através do download de *malwares* via aplicações ou links maliciosos, a par do surgimento de métodos mais atualizados. O CNCS (2023), considera os ataques *ransomware* mais ameaçadores do que, por exemplo, ataques mais tradicionais como o *phishing* e o *smishing.*

Kellerman e Murphy (2020), através do estudo *Modern Bank Heist* 3.0, referem que os ataques *Ransomware* ao setor financeiro aumentaram 9 vezes entre o mês de fevereiro e o mês de abril de 2020, portanto período inicial da pandemia da covid-19.

Segundo o relatório da ENISA (2023) sobre o cenário de ameaças, no período analisado (de abril de 2022 a julho de 2023), registou-se uma tendência ascendente de ataques *ransomware* justificado pelo bom retorno financeiro, sendo os cinco grupos de ataques *ransomware* mais comuns em todo o mundo foram *LockBit 3.0, BlackCat, BianLian, CL0P e Royal*. Esses grupos realizam ataques tanto com objetivo de oferecer serviços de *ransomware* RaaS (*Ransomware as a Service*) quanto para realizar chantagens cibernéticas. Ainda, de acordo com o mesmo relatório, os *links* URL e navegações em *web* são os métodos mais usados para realizar ataques *ransomware.*

2.3.2.2. MALWARE

Malwares ou *softwares* maliciosos, como também são conhecidos, são definidos pela ENISA (*2023*, pp.6) como "*any software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity or availability of a system*". Com isso, as principais caraterísticas dos ataques *Malware*

residem no facto de serem programas introduzidos num sistema sem o conhecimento do utilizador, com objetivos diversos dependendo das intenções do invasor, podendo ser o controlo de sistemas e redes (por exemplo, *botnets),* de dados (por exemplo, roubo de informações), ou até mesmo a indisposição total dos mesmos (DoS, em inglês *Denial of Services*).

Muito tem-se discutido sobre as formas de implementação dos *Malwares* nos sistemas, sendo que estes têm evoluído e acompanhado a evolução dos sistemas de informação e as medidas de segurança. De acordo com o último relatório *Thread Landscape* da ENISA (2023), uma das formas mais habituais de implementação *Malwares* em sistemas ao longo dos tempos tem sido através de macros[1] das ferramentas da Microsoft (Excel, Word e PowerPoint), sendo que foram bloqueados pela Microsoft como forma de combate aos ataques. Outros métodos mencionados utilizados na infeção de sistemas com *malwares* têm sido o acesso através de emails fraudulentos, ficheiros ZIP, PDFs e *Windows Script Files* (WSF).

Certo é que os atacantes tendem a copiar entre si técnicas já utilizadas, sendo de destacar a capacidade dos atacantes em criar, desenvolver e experimentar técnicas de implantação de *Malware* cada vez mais sofisticados e evoluídos, como referido anteriormente. O relatório destaca o aumento no uso de *comercial spywares*, que permitem que os atacantes obtenham acesso a sistemas usando ferramentas avançadas de "zero clique", ou seja, sem que os alvos tenham que interagir de qualquer forma. O objetivo desses *spywares* passa pela coleta de dados e informações dos utilizadores, sendo precisamente o roubo de informações e dados o principal objetivo dos cibercriminosos de *malware*. A *AgentTesla*, a *FormBook* e a *RedLine* foram identificadas como as maiores organizações responsáveis por ataques de *malware*, de acordo com o último *Threat Landscape* da ENISA (2023).

[1] Macros: uma ação ou um conjunto de ações que pode executar quantas vezes quiser; utilizada para automatizar tarefas que o utilizador faz repetidamente no Microsoft. (https://support.microsoft.com/pt-pt/office/guia-de-introdu%C3%A7%C3%A3o-criar-uma-macro-741130ca-080d-49f5-9471-1e5fb3d581a8)

2.3.2.3. ENGENHARIA SOCIAL (PHISHING E SMISHING)

De acordo com Instituto Nacional de Padrões e Tecnologias (NIST, 2015 *cit in* CNCS, 2023, pp. 101), a Engenharia Social consiste no "ato de enganar um indivíduo no sentido de este revelar informação sensível, assim obtendo-se acesso não autorizado ou cometendo fraude, com base numa associação com este indivíduo de modo a ganhar a sua confiança". Os principais aspetos desse tipo de ataque envolvem a intenção do invasor em induzir ou aproveitar-se de erros humanos ou comportamentos negligentes para obter acesso a dados ou serviços. Isso é feito por meio de várias formas de manipulação, e sempre requer alguma interação humana para ter sucesso. É importante observar que a Engenharia Social geralmente é utilizada pelos invasores para obter acesso inicial em sistemas (ENISA, *2023*).

De acordo com o mais recente relatório da ENISA sobre o cenário de ameaças (*ENISA*, 2023), entre as várias formas de Engenharia Social, destacam-se:

a) *Phishing*

Considerado pela FBI como o mais frequente crime de fraude digital, consiste numa técnica de engenharia social utilizada para roubar informações privadas de utilizadores através de anexos maliciosos e URLs infetados, enviados através de emails.

Também considerado como o ciberataque mais frequente nas seguradoras pelo relatório da União Europeia sobre ciberseguros, produzido pela Autoridade Europeia de Seguros e Pensões Ocupacionais (EIOPA, 2019, ppp.11) que carateriza o *phishing*

> this attack will typically direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. (EIOPA, 2019, pp.11)

Assim sendo, através desta técnica os atacantes procuram ludibriar os alvos com o objetivo de obter informações valiosas como credencias de login em redes sociais, aplicações de bancos, cartões de crédito, etc., tal como destacam Biswas, Mukhopadhyay, Kumar e Delen (2023). Os mesmos autores fazem ainda referência a ataques de *phishing* durante o período da Covid-19 em que atacantes visaram o desvio de fundos e ajudas financeiras nos EUA e no Reino Unido.

b) *Smishing*

O termo *Smishing* resulta da junção das palavras "SMS" e "*Phishing*" e ocorre quando os atacantes procuram coletar informações privadas ou convencer os alvos a abrir links maliciosos enviados através de mensagens de texto. "Tentativa por atacantes de obter dados pessoais, financeiros ou de segurança, por mensagem de texto" (Europol, 2018, *cit in* CNCS, 2023, pp. 103).

Basicamente, diferencia-se do *phishing* pelo seu *modus operandi*: enquanto o phishing distribui a isca através de emails, o *smishing* utiliza mensagens de textos.

No cenário português, o Centro Nacional de Cibersegurança (CNCS), através do último Relatório Cibersegurança em Portugal, considera os bancos a marca mais simulada pelos ataques de *phishing* (por email) juntamente com *smishing* (por SMS), sendo os clientes os mais afetados (CNCS, 2023). Vale referir que tanto o *phishing* como o *smishing* são considerados pelo CNCS tipos de ciberataque por si só e não subtipos de engenharia social.

c) *Vishing*

Uma outra modalidade dos ciberataques com recurso a engenharia social é o *Vishing* e trata-se da combinação entre "*Voice"* e "*Phishing"*, isto é, consiste na tentativa de extração de informações privadas de usuários através de técnicas de engenharia social, neste caso por chamadas telefónicas. "Uso de mensagens de voz ou de chamadas telefónicas para furtar identidades e recursos financeiros." (CNCS, 2023, pp.103)

Como mencionado anteriormente, os cibercriminosos têm acompanhado o desenvolvimento da tecnologia, sofisticando cada vez mais os ataques com a utilização de ferramentas cada vez mais atualizadas. A ENISA (2023), no seu relatório *Thread Landscape*, faz destaque a crescente tendência de utilizar ferramentas de Inteligência Artificial (IA), como o ChatGPT, em novas técnicas de engenharia social, devido à capacidade dessas ferramentas de imitar comportamentos humanos. Segundo o mesmo relatório, os invasores têm aproveitado das funcionalidades da IA para produzir emails de *phishing* com técnicas de linguagens cada vez mais aperfeiçoadas e próximas da linguagem humana, no que toca ao volume de texto, pontuação e comprimento das frases. Também a capacidade da IA em clonar vozes através de amostras recolhidas de redes sociais, tem sido explorada por cibercriminosos em ataques de *vishing*, para se

fazerem passar por amigos e familiares das vítimas para se obter informações privadas e financeiras principalmente. Assim, os cibercriminosos vêm a sua tarefa facilitada, já que o acesso às ferramentas de IA, por vezes disponíveis gratuitamente, permite a execução de ações maliciosas sem exigir conhecimentos técnicos avançados por parte deles, como destaca o CNCS (2023) no último Relatório de Cibersegurança em Portugal.

2.3.2.4. AMEAÇAS CONTRA DADOS

Cada vez mais a sociedade e as empresas vivem num mundo interconectado por meio de tecnologias e aplicações que produzem grandes quantidades de dados todos os segundos. Neste sentido, revela-se a grande importância dos dados, tanto é que é considerado dos recursos mais valiosos nos dias de hoje, o novo petróleo da atualidade (Clive Humby, 2006 *cit in* ENISA, 2023). De acordo com o último relatório *Thread Lanscape* (ENISA, 2023), o tratamento e a análise de dados são de grande importância para empresas que se apresentam competitivas no mercado, visto que permite a rapidez de processos, melhor gestão de clientes e a redução de custos fixos. Com isso, a procura por ferramentas que aprimoram o tratamento de dados e sua precisão está a levar as empresas a trocarem sistemas de *software* tradicionais baseados em algoritmos por sistemas baseados em IA com a capacidade quase autónoma de processar dados para a tomada de decisões. Devido a essa importância, os dados representam uma grande oportunidade para os cibercriminosos atingirem os alvos com vista a afetarem as operações dos sistemas, obterem ganhos financeiros, por exemplo.

As ameaças contra dados têm como objetivo bloquear o acesso a dados e/ou manipular dados com vista a interferir com o funcionamento normal do sistema e, de acordo com a ENISA (2023), podem ser classificadas em:

a) *Data Breach* (Violação de dados): consiste num ciberataque intencional e forçado contra um sistema com o objetivo de ganhar acesso e divulgar dados privados, protegidos e confidenciais.

b) *Data Leak* (Fuga de dados): trata-se de uma perda involuntária de dados privados, confidencias e protegidos provocada, por exemplo, por vulnerabilidades, falhas na segurança do sistema ou erro humano.

Estudos realizados pela Verizon (2023) e Tenable (2022) revelaram que as instituições financeiras (bancos e seguros) são o segundo tipo de instituições que mais sofrem violações de dados, conforme citado no relatório *Thread Landscape* da ENISA (2023).

2.3.2.5. AMEAÇAS CONTRA DISPONIBILIDADE

A necessidade de troca de informações e dados por parte de pessoas e instituições é uma das necessidades essenciais atualmente, sendo que as ameaças contra a disponibilidade são uma realidade e têm consequências significativas para os utentes quando é interrompida ou negada o seu acesso.

Uma das formas mais frequentes usada por cibercriminosos para negar ou interromper o acesso a sistemas e informações é a **Negação de Serviços** ou ***Distributed Denial of Service* (DDoS)**. Segundo a ENISA (2023), os ataques DDoS bloqueiam os utilizadores de sistemas o acesso a dados relevantes e serviços ao esgotar os recursos do serviço ou sobrecarregando a infraestrutura de rede do sistema.

No ponto de vista de Gupta e Dahyia (2021, *cit in* Silva & Ferrari 2023, pp.38), consideram ataque distribuído de negação de serviço

> um tipo de ataque distribuído que ocorre a partir de muitos computadores. O objetivo é sobrecarregar os sites/serviços online com mais tráfego do que o servidor ou a rede podem comportar. (Gupta & Dahyia, 2021 *cit in* Silva & Ferrari, 2023, pp.38)

Considerado um dos mais comuns ataques às tecnologias de informação, os ataques DDoS aumentaram de intensidade durante a pandemia da Covid-19, sendo que, de acordo com a ENISA (2023), o conflito entre a Rússia e a Ucrânia impulsionou os ataques DDoS, elevando-os a níveis sem precedentes.

Segundo a ENISA (2023) e confirmado pelo Relatório de cibersegurança em Portugal da CNCS (2023), os ataques DDoS tem-se verificado cada vez mais frequentes, duradouros, sofisticados e menos custoso, sendo que foram relatados em 2022 cerca de 13 milhões de ataques. Novas áreas, nomeadamente dispositivos móveis, têm sido explorados por cibercriminosos devido às suas limitações (por exemplo, bateria).

Contudo, os ataques DDoS nem sempre representam pontos negativos. O CNCS (2023), através do Relatório de cibersegurança em Portugal, enumera algumas utilidades positivas de ataques DDoS, nomeadamente, apoio a operações militares,

interrupção de atividades de organizações inimigas, demostração de força e intimidação e apoio em ações políticas.

As instituições financeiras (bancos e seguradoras) estão entre as indústrias mais impactadas por ataques DDoS, de acordo com estudos conduzidos pela F5Labs e StormWall, citados no relatório *Thread Landscape* (ENISA, 2023). Segundo a F5Labs, o setor dos serviços financeiros foi o segundo setor mais afetado depois das tecnologias, enquanto a StormWall considera o setor financeiro o mais afetado pelos ataques DDoS. De realçar a tendência ascendente dos ataques **Negação de Serviço por Resgate ou *Ransom Denial of Service*** (**RDoS**), que combina técnicas tradicionais de DDoS contudo com menos recursos, sendo por este motivo considerado mais perigoso do que o tradicional DDoS (ENISA, 2023). Por isso, este tipo de ataque tende a afetar entidades com sistemas menos robustos e vulneráveis, podendo ser executado de duas formas:

i) Primeiro implementa-se um ataque DDoS e depois pede-se um montante para que o ataque seja interrompido;

ii) Primeiro é enviado uma carta de extorsão com uma prova de possíveis danos da implementação do ataque e pede-se um resgate para não executar o ataque DDoS.

Outro método usado para ameaçar a disponibilidade de informações e dados prende-se no corte ao acesso à *Internet*, tendo em conta a sua importância no quotidiano quer para fins laborais, sociais, políticos ou lazer. **Ameaças à disponibilidade de *Internet*** são cortes no fornecimento da *internet* ou das comunicações eletrónicas, intencionais ou não, resultando em interrupções, *blackouts*, desligamentos ou censura na internet. (ENISA, 2023). Normalmente têm como alvo uma determinada população ou localidade, com vista a controlar a entrada e saída de informações, podendo ser causado por diretivas governamentais, cortes de energia e cabos, ciberataques, fenómenos naturais, ações militares, etc.

Os ataques à disponibilidade de Internet tendem a ser cada vez mais sofisticados e duradouros, alvejando populações específicas e momentos específicos, nomeadamente, crises humanitárias, conflitos e guerras. Um exemplo é o caso da Etiópia em que foi cortado o fornecimento de internet durante dois anos pelo governo por forma a impor o controlo, reduzir a democracia e ocultar violações de direitos de humanos (AccessNow, 2022 *cit in* ENISA, 2023).

Adelmann *et al.* (2020) chamam a atenção para o facto de interrupções prolongadas de serviços das instituições financeiras, juntamente com o comprometimento da integridade de dados, podem conduzir a perdas de confiança no setor financeiro, peça chave para o bom funcionamento da economia global.

2.3.2.6. MANIPULAÇÃO E INTERFERÊNCIA DE INFORMAÇÕES

Considerada pela ENISA (2023) como uma ameaça à cibersegurança, a **Manipulação de Informação** consiste numa ação legal, manipuladora, intencional e coordenada que ameaça ou tem potencial para influenciar negativamente valores, procedimentos e processos políticos. Essencialmente, a manipulação de informação põe em questão a veracidade de determinados conteúdos.

Pelo facto de a manipulação de informação afetar diretamente a integridade e veracidade da informação e, consequentemente, a tomada de decisões operacionais muitas vezes enganadas e erradas, é tratada como uma ameaça cibernética. Muitas vezes utilizada como um ponto de partida para ataques cibernéticos mais elaborados, a manipulação de informação deve merecer atenção por parte das entidades como um todo pois, o simples conhecimento por parte do departamento responsável pela cibersegurança sozinho não resolve o problema, mas sim, contribui para um ambiente mais fiável para a informação.

2.3.2.7. ATAQUES À CADEIA DE ABASTECIMENTO (SUPPLY CHAIN)

Ataques à cadeia de abastecimento ou ***Supply Chain Attacks*** como é mais conhecido, de acordo com um estudo realizado pelo Gabinete de Contabilidade do Governo Americano (US GAO, 2018), trata-se de ataques através do qual o invasor implementa vulnerabilidades em *hardwares* ou *softwares* de um sistema durante o seu processo de desenvolvimento, montagem ou *design*, com vista a tirar proveito dessas vulnerabilidades em momentos oportunos sem acesso direto por parte do atacante. Segundo a ENISA (2023), um *supply chain attack* carateriza-se pela junção de pelo menos dois ataques a agentes da cadeia de abastecimento: um primeiro ataque ao fornecedor do *software* ou *hardware* que é utilizado posteriormente num segundo ataque para ganhar acesso ao sistema do cliente final ou outro fornecedor.

O NIST (2012) destaca a importância de as empresas monitorarem as atividades de seus fornecedores de *hardwares* e *softwares* pois, partilhando da visão da ENISA (2023), os cibercriminosos cada vez mais reconhecem a influência dos fornecedores, pois um único golpe poderá afetar múltiplas organizações. Com isto, os atacantes aproveitam vulnerabilidades nos fornecedores para terem acesso aos sistemas da empresa, resultando na interrupção de suas atividades ou no acesso a informações privadas.

A crescente utilização e dependência de aplicações no quotidiano das instituições com vista a facilitar e agilitar processos (por exemplo, aplicações *internet banking*), poderá ser visto como vulnerabilidade nas instituições, tal como aponta a ENISA (2023). Cada vez mais é a interdependência entre aplicações utilizadas por organizações, podendo então ser afirmado que quanto maior o número de aplicações que possuir, maior é a vulnerabilidade da organização. Uma vez que a utilização destas aplicações, normalmente geridas por empresas externas de gestão de identidades, exige a autenticação de utilizadores por meio de suas credencias, faz com que estes fornecedores de gestão de identidades sejam um dos alvos a ter em conta por cibercriminosos. Neste sentido, Pollmeier *et al.* (2023) destacam a importância de as instituições financeiras supervisionar a forma como os próprios fornecedores de serviços gerem os seus *softwares*.

Outro meio vulnerável nas organizações, frequentemente considerado por vários autores o ativo mais valioso de uma empresa, é o capital humano, ou seja, os próprios funcionários. O último relatório sobre o cenário de ameaças da ENISA (2023) faz referência à utilização dos funcionários como ponto de entrada nos sistemas das organizações, exemplificando com casos em que cibercriminosos invadem computadores pessoais de funcionários através de *keylogger* (gravação de teclas pressionadas) e conseguem as credenciais do funcionário para obter acesso ao sistema da empresa. Este cenário foi potenciado pela Covid-19, levando a que grande parte dos funcionários trabalhassem "online" a partir de casa, o que representa uma oportunidade para os cibercriminosos atingirem os sistemas das empresas, como mencionado anteriormente pelo Diretor Adjunto do FBI, Paul Abbate, *cit in* Gulyás e Kiss (2023). Os funcionários mais visados pelos cibercriminosos tendem a ser os de maior influência e acesso nos sistemas, como os administradores. De acordo com um estudo realizado pela Deloitte (2022), as vulnerabilidades humanas são consideradas a principal ameaça à cibersegurança das empresas.

2.4. CIBERSEGURANÇA

Atualmente, os gestores e administradores das instituições estão cada vez mais atentos às questões relacionadas com os riscos de cibersegurança, considerado um sinal de fraqueza do sistema de controlo interno, devido às consequências significativas em termos de custos, multas e reputação, como destacam Masoud e Al-Utaibi (2022). A diretora do departamento de telecomunicações da União Internacional de Telecomunicações (ITU), Doreen Bogdan-Martin, destaca que, devido às necessidades de conectividade online impostas pela pandemia, a criação de um ciberespaço seguro tornou-se uma prioridade mais urgente do que nunca (ITU, 2021). Cada vez mais é reconhecida a importância da cibersegurança nas instituições financeiras, isto é, de ter a capacidade de proteger e defender o ciberespaço da empresa de ataques cibernéticos, que já é uma realidade bem presente (NIST, 2012).

Os autores Gulyás e Kiss (2023) afirmam mesmo que a preocupação para as instituições financeiras já não é "se serão ou não" alvos de ciberataques, mas sim "quando" vão ser atacados. Afirmação esta apoiada pela Autoridade Australiana de Regulamentação Prudencial (2020, *cit in* Pollmeier *et al.*, 2023), que refere a incidentes cibernéticos como uma certeza nas instituições financeiras, principalmente bancos.

Um estudo realizado por Pollmeier *et al.* (2023) demostra que o interesse na cibersegurança por parte dos órgãos de gestão dos bancos advém do desejo em manter a confiança dos clientes e não por causa das regulamentações impostas, nomeadamente quanto aos requisitos de capital. Sendo a salvaguarda de dados um dos principais fatores para a manutenção da confiança dos clientes, as instituições financeiras procuram dar garantias no que toca a segurança da informação.

2.4.1. ISO 27001

No sentido de garantir a salvaguarda das informações, surge a norma ISO 27001, uma norma internacional publicada em 2005 pela Organização Internacional de Normalização (ISO – *International Organization for Standardization*) que define um conjunto de princípios para a implementação de um Sistema de Gestão de Segurança de Informação (SGSI) eficaz, de acordo com Hsu, Wang e Lu (2016). Para Leite e Oliveira (2020) a norma ISO 27001 tem como objetivo fornecer fundamentos para estabelecer, implementar, manter e melhorar continuamente o SGSI de uma

organização, devendo o SGSI possuir quatro características essenciais: confidencialidade, integridade, disponibilidade e autenticidade. A Devoteam Cyber Trust (n.d.) carateriza o SGSI como um modelo holístico, uma vez que abrange todas as áreas de uma empresa no que trata a segurança da informação, desde a recursos humanos, proteção do meio físico, telecomunicações, etc.

A norma ISO 27001 conta, até ao momento com 3 versões: a primeira edição ISO 27001:2005, baseada na BS 7799-2, introduzida em 2005; em 2013, foi publicada uma segunda edição revisão da norma (ISO 27001:2013) com correções significativas; e a terceira edição, ISO 27001:2022, foi lançada em 2022 com pequenas correções no palavreado e revisões no Anexo A (IsecT Ltd., n.d.).

O normativo encontra-se estruturado em 11 tópicos e 1 anexo, de acordo com a consultora IsecT Ltd. (n.d.):

0. Introdução: descrição de um processo de gestão sistemática de riscos de informação.
1. *Scope*: requisitos genéricos para o estabelecimento de um SGSI em qualquer que seja o tipo, dimensão e natureza de empresa. “Que informações precisam de ser protegidas?”
2. Referências normativas.
3. Termos e Definições.
4. Contexto da organização: compreensão do contexto, das necessidades e das expetativas da empresa e dos *stakeholders*, por forma a definir o *scope*.
5. Liderança: demonstração de interesse e compromisso por parte dos órgãos de liderança para com o SGSI.
6. Planeamento: processos para identificar, analisar e planear o tratamento de riscos de informação.
7. Apoio: disponibilização de recursos adequados, aumento da consciencialização, preparação de documentações.
8. Operações: detalhes sobre métodos de avaliação e tratamento de riscos de informação, mudanças de gestão e documentações.
9. Evolução da performance: monitorização, quantificação, análise e revisão de processos, controlos e sistemas de gestão de segurança de informação.
10. Melhoria: tratamento de *findings* das auditorias e revisões.

Anexo A: a mais recente edição do Anexo A (ISO 27001:2022) consiste numa lista de 93 procedimentos de controlo de segurança, agrupados em medidas organizacionais, pessoas, físicas e tecnológicas. Segundo Kosling (2024) o tema organizacional inclui 37 medidas de controlo em relação à existência de políticas de segurança de informação, definição de responsabilidades e comprometimento com o SGSI, contacto com autoridades, ferramentas de monitorização de ameaças, controlo de acesso e identidade, gestão de ativos, entre outros. A categoria pessoas consiste em 8 medidas de controlo com foco nos colaboradores, considerados uma parte crítica na segurança de informação. Esta categoria engloba medidas como a triagem no processo de recrutamento, formação e consciencialização do pessoal, trabalho remoto, entre outros. As medidas físicas, consideradas tão importantes como as digitais, incluem 14 medidas de controlo nomeadamente áreas seguras, manutenção de equipamentos, utilidades de suporte, etc. Por último, as tecnológicas referem-se a um conjunto de 34 medidas de controlo sobre a proteção de *malware*, políticas de *backups*, monitorização de *login*, segurança da rede, e outros.

Embora obter a certificação ISO 27001 possa ser caro e demorado, podendo o processo chegar a 12 meses (Devoteam Cyber Trust, n.d.), de acordo com Hsu *et. al* (2016), uma instituição financeira certificada por esta norma é vista como proactiva e comprometida com a segurança da informação e dos dados. Portanto, as principais vantagens dessa certificação incluem o aumento da confiança dos clientes e a preferência de investidores, porém, de acordo com estudo realizado pelos mesmos autores, a adoção de uma boa segurança da informação, seguindo as diretrizes da ISO 27001 é visto pelas instituições mais como uma obrigação do que como uma oportunidade de vantagem competitiva. A Devoteam Cyber Trust (n.d.), através do portal informativo, acrescenta ainda algumas outras vantagens como maior fiabilidade e segurança da informação e dos sistemas, aumento do desempenho operacional das organizações, possibilidade de processos de melhoria contínua e aumento da eficácia organizacional através de um sistema de controlo de gestão. Todas essas vantagens são garantidas por meio de uma auditoria feita por uma entidade externa.

A consultora IsecT Ltd. (n.d.) chama a atenção pelo facto de uma certificação ISO 27001 válida é sim um sinal positivo, mas não uma certeza/garantia de segurança de informação. Garante a conformidade de um SGIS e não a proteção da informação.

2.4.2. Global Cybersecurity Index

Dado a crescente utilização e dependência das tecnologias de informação, a segurança cibernética tem se tornado uma prioridade global, como já mencionado anteriormente, surgindo a necessidade de ter ferramentas que permitem a avaliação e compreensão do estado da cibersegurança dos países. Neste sentido, em 2015, a ITU criou o *Global Cybersecurity Index* (GCI), um índice global que mede os níveis de comprometimento com a cibersegurança de países membros da ITU. O GCI tem o objetivo de ajudar na identificação e melhoria de áreas vulneráveis, promover a consciencialização global sobre as necessidades de cibersegurança e incentivar a adoção de boas práticas de cibersegurança, como referido no mais recente relatório da *Global Cybersecurity Index* 2020 (ITU, 2021).

De acordo com o mesmo relatório, a classificação dos países de acordo com o GCI baseia-se em cinco pilares de avaliação:

- **Medidas legais**: avalia a existência de legislações e regulamentos jurídicos que abordam assuntos ligados a cibersegurança e ao cibercrime. Legislações e regulamentos jurídicos permitem definir o que são considerados ilegalidades no ciberespaço e bem como os procedimentos para se fazer cumprir essas legislações e regulamentos jurídicos.
- **Medidas técnicas:** avalia as capacidades técnicas de um país, isto é, a existência de instituições e infraestruturas responsáveis por assuntos relacionado com a cibersegurança, nomeadamente a operacionalidade de uma equipa de resposta a incidentes informáticos (*Computer Incident Response Team* – CIRT). Também denominadas de equipas de resposta a incidentes de segurança informática (*Computer Security Incident Response Team* – CSIRT) ou equipas de resposta a emergências informáticos (*Computer Emergency Response Team* – CERT), são responsáveis por responder a incidentes de segurança cibernética nacionais através de ações sistemáticas e rápidas, aumentando a resiliência nacional. Importante

referir que podem existir CERTs nacionais (tratam da cibersegurança nacional) e CERTs setoriais (tratam da segurança cibernética de setores específicos).

- **Medidas organizacionais:** avalia as estratégias e políticas nacionais e organizacionais no que diz respeito a cibersegurança, nomeadamente a existência de uma Estratégia Nacional de Cibersegurança (ENC) e o compromisso dos órgãos executivos das instituições com a segurança cibernética. A ENC permite gerir de forma estruturada a cibersegurança nacional e deverá ser desenvolvida, implementada e executada numa perspetiva global do país, por forma a que as ações das instituições governamentais, do setor privado e da sociedade civil estejam alinhadas com o mesmo objetivo. Importante referir que a ENC deverá ser sempre revista e atualizada de acordo com os novos desafios da cibersegurança.
- **Medidas de desenvolvimento de capacidades:** avalia a existência de campanhas de sensibilização, programas de formação e educação, profissionais certificados e iniciativas no sentido de promoverem o desenvolvimento de capacidades de cibersegurança. Apesar das muitas vantagens sociais e económicas da digitalização, os riscos cibernéticos cresceram junto com essa evolução, podendo superar os benefícios da digitalização. Por isso, é crucial que todos, incluindo a sociedade e as instituições públicas e privadas, estejam conscientes dos perigos cibernéticos, devendo-se fortalecer as capacidades coletivas de cibersegurança para gerir esses riscos e proteger cidadãos, infraestruturas e empresas.
- **Medidas de cooperação:** avalia a existência de parcerias entre instituições (públicas e privadas), infraestruturas de cooperação nacional e redes de partilha de informações. Devido à conectividade de instituições e de infraestruturas, a cibersegurança é uma preocupação transnacional sendo por isso necessário a cooperação nacional, regional e internacional. A harmonização de medidas básicas de segurança, a partilha de informações e de boas práticas, são alguns dos principais objetivos da cooperação.

Tendo em conta os cinco requisitos acima descritos, o mais recente GCI foi realizado em 2020 e tendo em conta 193 países membros da ITU e o Estado da Palestina, através de um inquérito de 82 perguntas abordando os diferentes pilares. Os resultados ilustraram que os Estados Unidos da América é o país melhor classificado mundialmente com um *score* de 100, seguido do Reino Unido (*score* de 99,54) e da

Arábia Saudita (*score* de 99,54). Portugal, a nível mundial, alcançou um *score* de 97,32 ocupando a 14ª posição no *ranking*.

2.4.3. Recomendações

Vários autores têm feito recomendações às instituições financeiras no sentido de reforçarem a proteção do ciberespaço e minimizarem riscos cibernéticos, devido a sua grande importância no sistema financeiro global. De acordo com Adelmann *et al.* (2020) o foco deverá incidir sobre a prevenção, mitigação, quantificação e recuperação por forma a reduzir as vulnerabilidades, exigindo a necessidade de um esforço colaborativo de organismos de definição de normas, reguladores nacionais e internacionais, entre outros. Neste sentido, Leite e Oliveira (2020) destacam a criação da NIST *Cybersecurity Framework*, em 2014, um departamento da NIST que fornece apoio a nível internacional a organizações públicas e privadas através de normas, diretrizes e práticas em matéria de segurança cibernética com o objetivo de melhorar a capacidade de deteção e respostas a incidentes cibernéticos.

Adelmann *et al.* (2020) referem seis práticas para reduzir o risco cibernético para as instituições financeiras a nível global. São eles:

1. Análise de estabilidade financeira: melhoramento da capacidade de compreensão e mitigação de riscos através do mapeamento de principais interconexões entre estruturas financeiras e tecnológicas. Também, a quantificação de impactos potenciais de ataques cibernéticos proporciona uma melhor capacidade de resposta. A aplicação de 's*tress testing'* apresenta-se também como uma excelente ferramenta, utilizada por instituições financeiras para se estimar impactos de um possível ataque cibernético na liquidez e no capital.

2. Regulamentação e Supervisão: fortalecimento da cooperação internacional e adoção de boas práticas e normas por parte das instituições financeiras, nomeadamente comportamentos de '*cyber hygiene'*, o relato de incidentes, protocolos de resposta e recuperação, bem como procedimentos internos de governança. O objetivo passa essencialmente por reduzir riscos globais e encontrar soluções comuns para desafios compartilhados.

3. Resposta e Recuperação: cultivar hábitos de *'cyber hygiene'*, isto é, medidas de prevenção como a manutenção atempada de *softwares* e sistemas, com o objetivo

de fortalecer a capacidade de travar ataques e repor a normalidade do sistema ou serviço o mais rápido possível. Surge o conceito de resiliência cibernética, que se trata da capacidade de uma organização continuar a sua atividade, antecipando e adaptando-se a ameaças cibernéticas, através da resistência, contenção e recuperação de incidentes cibernéticos. Com o melhoramento da capacidade de resposta e recuperação, evita-se situações de crises financeiras, fortalecendo a resiliência do sistema financeiro global.

4. Partilha de informação: aprimorar a partilha de informações sobre ameaças cibernéticas entre setores público e privado para facilitar a resposta das instituições afetadas, pois a partilha de informação é uma das maiores fontes da mitigação de riscos. Torna-se essencial a partilha de informações quanto à origem e natureza de ameaças, relato de incidentes, boas práticas e técnicas de defesa.
5. Prevenção de ciberataques: reduzir as ameaças na sua origem através do aumento de esforços internacionais no sentido de partilha de informações e criação de protocolos de segurança cada vez mais atualizados, por forma a reduzir os custos e riscos para o setor financeiro, especialmente em economias em desenvolvimento consideradas as mais vulneráveis.
6. Desenvolvimento de capacidades: fortalecer a estabilidade financeira global e promover a inclusão tecnológica através do apoio financeiro e capacitação em economias em desenvolvimento, devendo essa ajuda ser uma prioridade para instituições financeiras internacionais. A conectividade desempenha um importante papel no desenvolvimento do mundo, o que foi claramente posto em evidência durante a Covid-19.

Tanto a ENISA (2023), como o CNCS (2023) enumeram um conjunto detalhado de recomendações e medidas a serem implementadas pelas instituições de acordo com tipologias de ataques cibernéticos.

Quadro 1: Recomendações por tipo de ciberataque

Ransomware
▪ Implementar uma estratégia de backup segura, seguindo procedimentos definidos e guardando-os em local secundário e *offline*;

▪ Garantir a segurança da infraestrutura de internet, realizando testes e rastreios de vulnerabilidades; ▪ Instalar e manter sistemas, aplicações e antivírus atualizados; ▪ Formação de cibersegurança periódica aos colaboradores; ▪ Assegurar uma configuração segura de tecnologias de acesso remoto; ▪ Colaborar com reguladores e divulgar informações sobre ataques de *ransomware* sofridos; ▪ Inventariar e controlar os ativos da instituição; ▪ Não utilizar dispositivos USB desconhecidos; ▪ Utilizar filtros para detetar e-mails maliciosos; ▪ Monitorizar as ações anteriores.
Malware
▪ Existência na teoria e na prática de um plano de resposta a incidentes; ▪ Colaborar com reguladores e comunicar informações sobre ataques de *malware* sofridos; ▪ Garantir a segurança da infraestrutura de internet, realizando testes e rastreios de vulnerabilidades; ▪ Formação de cibersegurança periódica aos colaboradores; ▪ Inventariar e controlar os ativos da instituição; ▪ Utilizar lista de permissões por forma a evitar a instalação de softwares sem permissão; ▪ Utilizar filtros para detetar e-mails maliciosos; ▪ Instalar sistemas de detenção de *malware* em todos os pontos de entrada/saída incluindo servidores, infraestruturas de rede, computadores e dispositivos móveis; ▪ Monitorizar as ações anteriores.
Engenharia Social (*Phishing, smishing e vishing*)
▪ Não abrir links e anexos de emails e SMS de origem suspeita; ▪ Não partilhar dados sensíveis por email, SMS ou telefonemas; ▪ Rever e atualizar planos de resposta de acordo com novas tendências; ▪ Realizar exercícios de simulação de *phishing/smishing/vishing;* ▪ Conhecer e ter atenção a domínios semelhantes ao da instituição; ▪ Formação de cibersegurança personalizada aos departamentos de RH, vendas, finanças, IT e segurança de informação; ▪ Assegurar relatos fiáveis sobre as infraestruturas alvos de ataques de engenharia social, por forma a apoiar em possíveis investigações; ▪ Instalar instrumentos de inteligência que permitam a identificação de ameaças e a transformação da informação em mecanismos de prevenção e defesa; ▪ Proibir a troca de imagem de disco por email; ▪ Bloquear a possibilidade de permissão de acesso e execução de softwares a terceiros; ▪ Utilizar instrumentos que notificam a receção de email de utilizador desconhecido;

▪ Monitorizar as ações anteriores.
Ameaças contra dados
▪ Ter um departamento especializado no combate ao vazamento de dados por forma a salvaguardar a disponibilidade, confidencialidade e integridade dos dados; ▪ Construir plano de mitigação tendo em conta os ativos que podem ser visados por ciberatacantes e uma boa avaliação dos riscos; ▪ Planeamento e orçamento adequado para riscos de gestão de dados; ▪ Política de gestão de autorizações que reveja o acesso de cada funcionário de acordo com os poderes e presença na organização; ▪ Seguir políticas de confiança zero: "nunca confiar, sempre verificar" especialmente quando se trata de informações sensíveis; ▪ Existência de *passwords* únicas e fortes para cada sistema por forma a evitar que uma única violação de dados comprometa vários sistemas; ▪ Existência de autenticação multifatorial para fortalecer o acesso aos sistemas; ▪ Formação de cibersegurança a todos funcionários, tanto do departamento de segurança de informação como os utilizadores finais; ▪ Realizar auditorias à segurança de dados; ▪ Realizar backups de dados, guardados em locais distintos por forma a evitar que um único acontecimento (ataque, desastre natural, etc.) afete todos os backups.
Ameaças contra disponibilidade
▪ Ter uma equipa preparada para dar resposta a incidentes de DDoS; ▪ Ter um plano de contingência para repor rapidamente os serviços essenciais da instituição e reduzir o tempo necessário para retornar à normalidade; ▪ Construir plano de mitigação tendo em conta os ativos e serviços que podem ser visados por ataques de DDoS e uma boa avaliação dos riscos; ▪ Manter o sistema sempre atualizado e corrigir possíveis vulnerabilidades; ▪ Investir em infraestruturas e sistemas mais potentes, como a nuvem e sistemas com maior banda larga, por forma a que ataques DDoS bem-sucedidos sejam mais difíceis e custosos; ▪ Formação de cibersegurança aos funcionários.
Manipulação e interferência de informação
▪ Promover trocas de informações com organismos contra manipulação de informação; ▪ Melhorar a qualidade e a disponibilidade de dados sobre a manipulação de informação, nomeadamente aspetos de cibersegurança como técnicas usadas; ▪ Ações de sensibilização no sentido de limitar a utilização de conteúdos que possam comprometer infraestruturas dentro da organização; ▪ Cultivar processos críticos de triagem de informações, considerando a autenticidade das informações, com o objetivo de mitigar riscos; ▪ Detetar e mitigar informações manipuladas fornecidas por redes sociais, isto é, suspender contas falsas, filtrar noticias falsas, reduzir atividades automatizadas.
Supply chain attack

- Ter um programa de gestão de riscos cibernéticos da cadeia de abastecimentos da instituição e, bem como, um serviço de gestão de riscos terceirizado;
- Levar em conta os principais fornecedores nos planos de respostas a incidentes cibernéticos;
- Não reutilizar passwords em fornecedores de produtos e serviços;
- Criar defesas baseadas no princípio de que o sistema será invadido;
- O acesso físico aos dispositivos deverá ser igualmente restrito, assegurando que a segurança física e a segurança cibernética estejam alinhadas;
- Investigar fornecedores além dos hardwares/softwares e produtos, não confiar somente na documentação;
- Inventariar os fornecedores de softwares, hardwares e serviços confiáveis, evitando a conexão de fontes desconhecidas;
- Política de pouca tolerância nas relações com fornecedores que apresentam produtos falsificados e fora do acordado contratualmente;
- Assegurar que todos os *firmwares* e *drivers* ligados ao sistema são seguros;
- Maior controlo no acesso dos fornecedores de serviço, através de comunicações criptografadas e autenticação multifatorial.

***Fonte**: Adaptado de ENISA (2023, ppp.140) e CNCS (2023, ppp.92)*

Devido ao grande impacto que a pandemia da Covid-19 teve no aceleramento da digitalização dos serviços financeiros e no panorama da cibersegurança das instituições financeiras, a Deloitte (2022) realizou um estudo e enumerou um conjunto de quatro conclusões para as instituições financeiras reforçarem as suas estruturas de cibersegurança:

1. Implementar de forma definitiva algumas medidas adotadas anteriormente a curto prazo, nomeadamente o trabalho remoto e a disponibilização de produtos e serviços digitais;
2. Reforma de sistemas tradicionais, uma vez que dificilmente acompanharão a transformação digital. O amadurecimento de infraestruturas cibernéticas, a adoção de boas práticas cibernéticas e existência de pessoal capacitado nas instituições são igualmente importantes no processo de transição digital segura das instituições;
3. Fortalecer mecanismos de controlo e deteção através da adoção de políticas de "nunca confiar, sempre verificar", digitalização de funções cibernéticas com maior agilidade e rapidez na resposta;
4. Aumento de investimento em cibersegurança e iniciativas de formação de funcionários, uma vez que continuam a ser a maior vulnerabilidade das instituições.

2.4.4. Contexto da cibersegurança em Cabo Verde

Em um mundo cada vez mais conectado, a digitalização revela-se como uma peça chave nos vários componentes deste sistema. Tal como o mundo, Cabo Verde tem evoluído e acompanhado a era digital, procurando a digitalização de diversos sectores, sendo a economia um deles. A crescente utilização e dependência das tecnologias de informação são já uma realidade na economia cabo-verdiana, sendo considerada a "espinha dorsal das economias modernas" principalmente devido ao aumento da eficiência organizacional (Resolução nº 21/2016, 2016, pp. 531). Por este motivo, Cabo Verde tem investido na transformação digital, sendo que esta transformação só é possível num ambiente seguro para os utilizadores e os cidadãos em geral, ilustrando uma vez mais a importância da cibersegurança para o desenvolvimento de um país. "Impossível falar-se de tudo o que é economia digital sem que as pessoas se sintam seguras para fazer negócio" afirma Pedro Lopes, Secretário de Estado de Cabo Verde para a Economia Digital, em declaração à Rádio Morabeza (Martins, 2023).

Segundo a Resolução nº21/2016 (2016, pp. 548), a cibersegurança trata-se do "conjunto de ações que permitem a um estado suportar eventos de ciberespaço que podem comprometer a disponibilidade, integridade ou confidencialidade dos dados armazenados, processados ou transmitidos."

De acordo com o Decreto-lei nº 9/2021 (2021), a segurança cibernética atualmente tem um papel tão importante quanto à segurança física numa sociedade, sobretudo devido às consequências dos ataques ao ciberespaço, nomeadamente a perda de confiança dos cidadãos. Durante um debate na Rádio Alfa acerca do cibercrime em Cabo Verde, Hélio Africano, ativista digital, afirma que apesar de Cabo Verde estar a dar grandes passos na era digital, o país não transpôs as mesmas preocupações da segurança física para a segurança cibernética, isto é, a cibersegurança não tem acompanhado a velocidade da digitalização do país. Péricles Pinto, administrador da empresa Sky Tech, exemplifica com o caso do investimento de Cabo Verde no cabo EllaLink em 2021 para aumentar a capacidade do país na transmissão de dados (Rádio Alfa CV, 2023).

2.4.4.1. INDICADORES GCI

De acordo com o último Índice Global de Segurança Cibernética GCI 2020, Cabo Verde encontra-se na posição 136 a nível global e na posição 27 a nível do continente

africano. Importante referir que o país tem mostrado um compromisso crescente por forma a reduzir os riscos cibernéticos, investindo num ciberespaço cada vez mais seguro para os utentes, sobretudo após a Covid-19. Prova disso é o facto de Cabo Verde subir 27 posições no GCI 2020 face à edição anterior. (ITU, 2021)

Por forma a melhor analisar o contexto da cibersegurança em Cabo Verde, a análise será feita de acordo com os cinco pilares do GCI, índice sobre a cibersegurança desenvolvida pela ITU e que já foi abordada anteriormente neste trabalho (2.4.1 ISO 27001).

O **primeiro pilar** do GCI aborda as medidas legais do país. Cabo Verde, em termos de legislação na matéria de cibersegurança, encontra-se bem avaliado. Quem o diz é o diretor de segurança e *compliance* da NOSI (empresa responsável pela gestão e cibersegurança da rede privativa do Estado de Cabo Verde), Engenheiro Adilson Rodrigues, através do debate sobre o cibercrime em Cabo Verde (Rádio Alfa CV, 2023). As principais legislações e regulamentos que regem matérias ligadas ao cibercrime e à cibersegurança são:

- Lei nº 8/IX/2017: denominada lei do cibercrime, foi publicada a 20 de março de 2017 e atua em três grandes áreas: primeiro, contém normas penais que definem as ações consideradas crimes no ciberespaço nacional; segundo, estabelece os procedimentos investigativos a serem seguidos pela ordem de polícia criminal; e por último, define mecanismos de cooperação nacional (público e privado) e internacional.
- Decreto-Lei 9/2021: publicada a 29 de janeiro de 2021, estabelece o Regime jurídico cabo-verdiano para a cibersegurança com o objetivo de promover a segurança das redes e dos sistemas de informação. O regime define a estrutura de segurança do ciberespaço de Cabo Verde, nomeadamente o Núcleo Nacional de Cibersegurança (NNCS), o Centro Nacional de Cibersegurança (CNCS) e a *Computer Emergency Response Team* de Cabo Verde (CV-CERT) e as respetivas competências.
- Decreto-Regulamentar 1/2021: também publicada a 29 de janeiro de 2021, este decreto regulamentar visa essencialmente fornecer as bases para a operacionalização da CIRT. Define as suas funções e os procedimentos, a sua estrutura e composição e o seu órgão administrativo.

- Resolução 21/2016: publicada a 7 de março de 2016, a Resolução 21/2016 define a Estratégia Nacional para Cibersegurança (ENC), seus objetivos e a duração para a sua implementação. Através dessa Resolução criou-se também o NNCS, como responsável pela implementação da ENC, especificando a sua composição, sua missão e as suas atribuições.
- Lei nº 133/V/2001: estabelece o Regime Jurídico geral de proteção de dados pessoais, foi publicada em 22 de janeiro de 2001 e posteriormente revista pela lei 41/VIII/2013 em 17 de setembro de 2013. O Regime Jurídico geral de proteção de dados estabelece os princípios, direitos e obrigações relativos ao tratamento automatizado e não automatizados de dados pessoais e bem como a definição da entidade responsável pela fiscalização e garantia do regime, a CNPD (Comissão Nacional de Proteção de Dados).
- Decreto-Lei nº 44/2009: de 9 de novembro de 2009, este decreto-lei estabelece a Infraestrutura de Chaves Públicas de Cabo Verde. Esta legislação é importante para assegurar a segurança, confidencialidade e integridade da informação, nomeadamente para a emissão de certificados digitais, realização de transações eletrónicas e assinaturas eletrónicas de transações e documentos eletrónicos.
- Decreto-Lei nº 33/2007: com objetivo de rever o regime da assinatura digital de 2003, foi publicada em 24 de setembro de 2007 o decreto-lei nº33/2007 para regular a assinatura eletrónica (terminologia adotada em substituição ao antigo regime), a sua eficácia jurídica e os contratos celebrados por via eletrónica. O decreto-lei é regulamentado pelo Decreto-Regulamentar nº 18/2007.
- Decreto-Lei nº 27/2023: publicada recentemente a 20 de outubro de 2023, este decreto-lei trata de assuntos relacionados com o reconhecimento e aceitação de meios de identificação eletrónica de pessoas singulares e coletivas. A validação, eficácia e veracidade de documentos eletrónicos, bem como a prestação de serviços eletrónicos também são tratados ao longo do diploma.
- Regime Jurídico dos Serviços Digitais e Comércio Eletrónico: sabe-se que a proposta de lei foi aprovada pelo parlamento na generalidade no dia 26 de janeiro de 2024 e aprovada na especialidade a 19 de junho do mesmo ano, sendo desconhecida até à data do presente trabalho a sua publicação no Boletim Oficial da República de Cabo Verde. Este regime visa essencialmente reforçar a segurança do comércio eletrónico tanto para os operadores como para os consumidores,

> garantindo o respeito dos direitos dos consumidores e estabelecendo regras, princípios e obrigações dos operadores e comerciantes. (Governo de Cabo Verde, 2024a, 2024b)

Quanto ao **segundo requisito** da GCI, que são as medidas técnicas, Cabo Verde tem mostrado alguma fragilidade e debilidade, sendo considerada uma área potencial de melhoria (ITU, 2021). Uma das principais exigências deste pilar prende-se com a existência de uma CIRT nacional, que segundo o Decreto-Regulamentar nº1/2021 (2021), "são equipas ou entidades centralizadas, que têm como principais objetivos a prevenção, identificação, gestão e resolução de problemas relacionados com a segurança informática de forma rápida e eficiente" (p. 207). A CIRT é importante uma vez que permite monitorizar de forma centralizada as tecnologias e os sistemas de informação, detetar e responder em tempo útil e metodicamente possíveis ataques no ciberespaço. Além disso permite a construção de conhecimentos e tomada de medidas preventivas com base nas investigações e relatórios pós-incidentes.

Apesar do país ter legislações muito claras, desde 2021, para a criação da CIRT/CV-CERT (Decreto-Lei 9/2021 e Decreto-Regulamentar 1/2021), até à data da realização deste estudo não foram encontrados dados que comprovam a operacionalização na prática desta equipa. O próprio Decreto-Regulamentar nº1/2021 (2021) destaca a necessidade urgente de implementar a CIRT, mesmo antes da criação do CNC, devido à carência de uma equipa robusta no país capaz de lidar com incidentes cibernéticos, especialmente considerando os investimentos do país na evolução digital e a tendência crescente de ciberataques mundialmente. Durante um debate sobre o cibercrime em Cabo Verde (Rádio Alfa CV, 2023), Péricles Pinto, administrador da Sky Tech, reafirma essa necessidade do país em ter uma entidade capaz de dar uma resposta "unificada e em tempo útil" a ataques cibernéticos, construir conhecimento através do estudo do *modus operandi* desse ataque e prevenir futuros ataques com o mesmo *modus*.

Em relação ao **terceiro pilar**, medidas organizacionais, importa referir que Cabo Verde possui uma ENC estipulada desde 2016 pela Resolução nº 21/2016 (2016), que deveria ser coordenada e implementada pelo NNCS até 2019. De acordo com o mesmo diploma, a ENC do país desdobra-se em quatro grandes objetivos:

1) **Criar o CNCS**: uma entidade nacional responsável pela cibersegurança nacional através das suas componentes estratégicas, técnica e operacional;
2) **Garantir a segurança cibernética das infraestruturas críticas nacionais**: tendo em conta que um ataque à uma infraestrutura crítica (saúde, transporte, comunicação, financeiro, etc.) poderá trazer consequências humanas e económicas graves para o país, a garantia da cibersegurança dessas infraestruturas é uma prioridade para a cibersegurança nacional;
3) **Garantir a cibersegurança na defesa nacional**: criação de políticas de cibersegurança e garantir a capacitação de agentes públicos para a defesa da soberania nacional;
4) **Garantir a segurança dos cidadãos no ciberespaço**: tendo em conta que a garantia da cibersegurança nacional resulta de um esforço coletivo de todos, incluindo cidadãos, garantir a consciencialização dos mesmos sobre riscos cibernéticos e técnicas de proteção é de extrema importância para uma vertente preventiva da cibersegurança nacional. Numa vertente repressiva, é importante legislar e capacitar instituições de segurança e judicial em matéria de cibercrime, por forma a que os cidadãos se sintam protegidos no ciberespaço.

Apesar do país ter uma estratégia bem delineada desde 2016, com objetivos bem definidos, a verdade é que até à data da realização deste estudo os objetivos da ENC de Cabo Verde ainda não foram conseguidos, tal como confirma o diretor de segurança e *compliance* da NOSI, Adilson Rodrigues, através do debate sobre o cibercrime em Cabo Verde (Rádio Alfa CV, 2023), justificando tal atraso com a mudança de poder no governo em 2016. O mesmo afirma ainda que Cabo Verde não possui até à data uma entidade especializada para garantir a cibersegurança do país, que deveria ser a CNCS.

Quanto ao **quarto pilar**, medidas de desenvolvimento de capacidades, o país é avaliado com um *score* relativamente baixo no GCI (1,96 de 20). É reconhecida a necessidade do país em investir na sensibilização e consciencialização das instituições e dos cidadãos em matérias relacionadas com a cibersegurança e os riscos da utilização dos meios digitais. Os recursos humanos são considerados os meios mais vulneráveis das organizações, por diversos autores como já referido anteriormente, e Cabo Verde não é exceção a regra tal como afirma Hélio Africano, ativista digital, no debate sobre

cibercrime em Cabo Verde (Rádio Alfa CV, 2023). O mesmo destaca a falta de literacia digital nacional, isto é, a não inclusão de assuntos como a cibersegurança e digitalização no ensino escolar, considerada uma importante ferramenta de mitigação de riscos cibernéticos. No mesmo debate, Emanuel Livramento, engenheiro da Agência de Regulação Multissectorial da Economia (ARME), reafirma a necessidade de mais ações de sensibilização no país sendo que a instituição tem realizado, em parceria com outras instituições, ações de sensibilização em matéria de cibersegurança, a nível do ensino básico, exemplificando com o lançamento da quinta edição da cartilha Proteção das crianças no ciberespaço. Outra instituição que tem desempenhado um papel importante no sentido de promover a cibersegurança nacional em Cabo Verde é a NOSI que, de acordo com o diretor de segurança e *compliance*, Adilson Rodrigues, tem realizado iniciativas nesse sentido, nomeadamente a WebLab, que é um programa escolar opcional realizado em parceria com o ministério de educação que implementa laboratórios informáticos em todas as escolas secundárias, e são ministrados um conjunto de temas, sendo um deles a cibersegurança. Refere-se também à NOSI Academy, um programa de estágio de seis meses para recém-licenciados que inclui capacitação em cibersegurança. Além disso, menciona os TechParks, dois parques tecnológicos concebidos para promover o desenvolvimento digital e tecnológico do país e onde já foi realizada uma importante ação de capacitação em matéria de cibercrime para técnicos de diversas instituições críticas do país.

Portanto, verifica-se uma tendência cada vez mais crescente do país em investir na sensibilização e capacitação das instituições e dos cidadãos, sendo que ainda é reconhecida alguma fragilidade do país no que toca à consciencialização dos cidadãos e à existência de técnicos capacitados e especializados em cibersegurança, ficando o país dependente de soluções internacionais, como defende Péricles Pinto ao longo do debate sobre cibercrime em Cabo Verde (Rádio Alfa CV, 2023).

No que toca ao **quinto e último pilar** da GCI, medidas de cooperação, de acordo com o último GCI (ITU, 2021), é mencionado como ponto relativamente forte de Cabo Verde. Tendo em conta que o assunto da cibersegurança é transversal, isto é, existe a possibilidade de cibercriminosos que estejam fora do território nacional atacar o ciberespaço de Cabo Verde e, de acordo com Adilson Rodrigues durante o debate sobre o cibercrime em Cabo Verde (Rádio Alfa CV, 2023), sabendo que a jurisdição de Cabo Verde só permite investigar incidentes dentro do território nacional, a cooperação

internacional é então de extrema importância para o país. Neste sentido, Cabo Verde aderiu em junho de 2018 à Convenção de Cibercrime, mais conhecida como Convenção de Budapeste, que é um tratado de direito penal internacional e de direito processual penal que define os crimes cometidos através da internet e as respetivas ações penais, como refere em comunicado o Ministério das Finanças de Cabo Verde (2021). Em 2020, Cabo Verde ratificou a Convenção de Malabo, uma convenção da União Africana para a Cibersegurança e Proteção de Dados Pessoais com o objetivo de tratar legalmente assuntos como o comércio eletrónico, proteção de dados e cibersegurança no continente africano, de acordo com informações da Data Protection Africa (2023). Além disso, o país aderiu à Convenção 108 do Concelho Europeu destinada à Proteção de Dados Pessoais, uma convenção que visa proteger as pessoas no tratamento dos seus dados pessoais, salvaguardando os direitos humanos e liberdades fundamentais (Conselho Europeu, 2018). De acordo com o Eng.º da ARME, Emanuel Livramento, a adesão às convenções internacionais é importante pois, permite à Cabo Verde acionar mecanismos internacionais de cooperação e apoio, incluindo requisitar evidências de determinados ataques internacionais.

Portanto, a nível de cooperação internacional o país tem mostrado alguma robustez, sendo que urge a necessidade de uma entidade própria para promover tanto a cooperação internacional como a cooperação regional no país, como destaca Emanuel Livramento (Rádio Alfa CV, 2023). De acordo com o ativista Hélio Africano, Cabo Verde tem mostrado fragilidades na cooperação regional uma vez que não existe uma estrutura organizada para realizar investigações, promover a partilha de informações e a aprendizagem em tempo útil com ataques já registados em instituições do país, como foi o caso dos ataques à Rede Privativa do Estado e à Telecom SA.

3. METODOLOGIA

Após realizar uma importante revisão da literatura existente em relação ao tema, por forma a melhor contextualizar com assuntos ligados aos riscos cibernéticos e a cibersegurança, passa-se agora à apresentação dos elementos da investigação. De acordo com Hill e Hill (2009), qualquer investigação deverá conter objetivos, escolha do tema, planeamento dos métodos de recolha de dados e análise desses dados. Esses pontos correspondentes ao presente estudo serão apresentados a seguir. O estudo consiste na avaliação de estratégias de mitigação de riscos cibernéticos numa instituição financeira, neste caso a Caixa Económica de Cabo Verde (CECV).

3.1. MÉTODO DE INVESTIGAÇÃO

Para que uma tarefa seja realizada de forma bem-sucedida, é necessário seguir um conjunto de processos ordenados que visam alcançar um objetivo final específico, isto é um método. De acordo com Cervo e Bervian (2002, pp. 24), no âmbito da investigação, um método representa "o conjunto de processos empregados na investigação e na demostração da verdade".

Para a realização da investigação pretende-se fazer um Estudo de Caso uma vez que se pretende estudar um conjunto de decisões de uma organização, nomeadamente por que são tomadas, como são implementadas e com que resultado (Schramm, 1974, *cit in* Yin, 2010). De acordo com Yin (2010), o estudo de caso permite analisar as caraterísticas globais e significativas de processos organizacionais, pelo que se adequa aos objetivos da investigação, tratadas no tópico a seguir.

3.2. OBJETIVOS DE INVESTIGAÇÃO

Tendo em conta a revisão de literatura sobre os riscos cibernéticos e a cibersegurança, a tendência crescente de ataques cibernéticos às instituições financeiras, principalmente aos bancos, é já uma realidade mundial. Com isso, o objeto do estudo será a avaliação das estratégias de mitigação de riscos cibernéticos da CECV, incluindo o estudo dos desafios e benefícios do processo de certificação da instituição com o ISO 27001. Assim, foram definidos como objetivos do estudo:

- Avaliar a eficácia das estratégias de mitigação de riscos cibernéticos da CECV;
- Identificar custos, desafios e benefícios da certificação ISO 27001;
- Identificar vulnerabilidades e propor melhorias.

3.3. TÉCNICA DE RECOLHA DE DADOS

Após ser definido o assunto da investigação, a revisão da literatura e os objetivos, procede-se a coleta de dados que, de acordo com Cervo e Bervian (2002), trata-se de uma tarefa importante que envolve passos desde a definição da população a ser estudada, os instrumentos de coleta, a programação da coleta até a própria coleta.

Para Yin (2010), a utilização de múltiplas fontes de dados resulta em melhores estudos de caso principalmente devido à possibilidade triangulação de informações, não recomendando, portanto, a utilização de fontes individuais. Seguindo esta linha de raciocínio, para a realização deste estudo vão ser utilizadas três técnicas de recolha de dados:

a) Entrevistas: consiste numa conversa, através de um interrogatório do informante, com o objetivo de recolher dados para a pesquisa (Cervo & Bervian, 2002). Por ser um contacto direto do investigador com o entrevistado, a entrevista traz vantagens em relação a outras técnicas, como os questionários, uma vez que permite registar observações sobre a aparência, sobre o comportamento e sobre as atitudes do entrevistado, além de permitir maior autenticidade, flexibilidade e profundidade das informações, tal como acrescenta Quivy e Campenhoudt (1998). Foram aplicadas entrevistas não-estruturadas, uma vez que as perguntas são abertas e o entrevistador poderá conduzir a entrevista da maneira que for mais adequada, por forma a obter respostas mais amplas (Marconi & Lakatos, 2003). Contudo, as entrevistas são não-estruturadas, mas focalizadas, visto que, de acordo com Ander-Egg (1978, *cit in* Marconi & Lakatos, 2003) há um guião com perguntas pré-definidas, mas que poderá não ser seguida de forma rigorosa. Quivy e Campenhoudt (1998) conjuga esses dois conceitos anteriores e refere-as como entrevistas semidirigidas ou semiestruturadas, visto que não se trata de entrevistas inteiramente abertas, mas com uma serie de perguntas-guias que poderão não ser aplicadas pela ordem, deixando o entrevistado à vontade para falar abertamente, mas procurando sempre o investigador redirecionar a entrevistas para os objetivos da investigação.

b) Questionários: considerada por Cervo e Bervian (2002) como a técnica mais utilizada para a coleta de dados, pois permite medir com maior exatidão os elementos desejados. Marconi e Lakatos (2003) definem os questionários como sendo instrumentos de coleta de dados, compostas por perguntas ordenadas que deverão ser respondidas sem a presença do entrevistador e em anonimato. Os mesmos autores destacam a importância de os questionários conterem informações sobre a natureza da pesquisa, a sua importância e a necessidade de obter respostas. As principais vantagens desta técnica são a economia de tempo e pessoal no trabalho de campo, maior alcance de pessoas e dados, e maior liberdade e segurança dos participantes devido ao anonimato. Os questionários aplicados durante o estudo contêm perguntas maioritariamente fechadas, mas também algumas abertas, seguindo a lógica de Quivy e Campenhoudt (1998), que destacam a maior obtenção de informações sobre o assunto através dessa combinação. De acordo com Cervo e Bervian (2002), as perguntas fechadas são padronizadas, permitindo a obtenção de respostas mais precisas e fáceis de analisar, enquanto as perguntas abertas se destinam a obtenção de respostas mais livres, ricas e variadas, sendo mais difíceis de serem analisadas. Os questionários aplicados são designados de administração direta uma vez que são os próprios inquiridos a preencher os questionários.
c) Recolha de documentos.

3.4. MÉTODO DE SELEÇÃO DE DADOS

Segundo Quivy e Campenhoudt (1998, pp. 159) para se estudar "o modo de funcionamento de uma empresa será necessário, na maior parte das vezes, interrogar os que dela fazem parte, ainda que o objeto de estudo seja constituído pela própria empresa, e não pelas pessoas". Seguindo esta linha de pensamento e os objetivos de estudo, foram definidos os seguintes métodos de seleção de dados:

a) Entrevistas: tendo em conta a localização geográfica dos entrevistados e a sua disponibilidade, foram realizadas duas entrevistas, online, através da plataforma Zoom: uma delas a um profissional do departamento de Informática, Comunicação e Segurança da CECV (designada ao longo do estudo por **I1** – Indivíduo 1), sendo a outra realizada, em conjunto, a dois profissionais administradores de rede da CECV (designados ao longo do estudo por **I2** – Indivíduo 2 e **I3** – Indivíduo 3). Os

profissionais selecionados são de áreas específicas, relacionadas diretamente com os objetivos do estudo e cujas informações extraídas são extremamente valiosas para o sucesso do estudo. Tal como destacam Quivy e Campenhoudt (1998), o contacto direto com profissionais de áreas ligadas diretamente ao tema de investigação possibilita retirar informações muito ricas através da expressão das perceções dos entrevistados, possibilitando ao investigador um elevado grau de autenticidade e profundidade.

b) Questionários: foram aplicados dois questionários online através da plataforma *Google Forms*, destinados aos colaboradores e clientes (particulares e empresas) da instituição. Tendo em conta que a instituição conta com um universo de 364 colaboradores ativos e com mais de 300.000 clientes particulares e empresas (CECV, 2023), foi necessário definir-se duas amostras, isto é, partes representativas dos universos de casos que, após análise dos dados destas partes, permitirá retirar conclusões e serem extrapoladas para os universos (Hill & Hill, 2009).

   Tendo em conta que é conhecida a fraca adesão dos colaboradores da instituição a questionários e a não possibilidade de a instituição distribuir pelos seus canais questionários a clientes fora do âmbito de atividade do banco, decidiu-se por amostragens por conveniência definida por Hill e Hill (2009) como sendo um método de amostragem não-casual ou não-probabilístico em que os casos escolhidos são os de fácil acesso, trazendo, portanto, vantagens como a rapidez e a facilidade de alcance. Contudo apresenta como principal desvantagem a falta de confiança na extrapolação dos resultados da amostra para o universo, pois não há garantias que a amostra seja representativa do universo de casos. Quivy e Campenhoudt (1998) destacam o frequente estudo de componentes que não sejam estritamente representativas, mas são características da população, como uma das alternativas mais frequentes quando não se consegue estudar toda a população. Com isso, o questionário destinado aos colaboradores foi distribuído de forma massiva na instituição por forma a obter o maior número de respostas possíveis. Quanto ao questionário aplicado a clientes, foi distribuído pelo próprio investigador através de redes sociais e contactos, sobretudo a amigos e conhecidos. Devido a natureza de distribuição dos questionários, especialmente a dos colaboradores, pode-se considerar que contenha elementos de uma amostragem casual aleatória simples

uma vez que todos os colaboradores tiveram oportunidades iguais de serem incluídos na amostra (Hill & Hill, 2009).

Importante referir que, depois de elaborados os questionários, estes foram submetidos a uma fase de pré-testes, que segundo Marconi e Lakatos (2003) permite identificar eventuais falhas, testar o vocabulário, verificar a dimensão e adequar a linguagem antes de ser distribuído em definitivo. Os questionários foram enviados para a análise e revisão do orientador da investigação, submetidos à aprovação do responsável de comunicação, informática e segurança da instituição em estudo e aplicados a dois particulares.

c) Documentos: foram selecionados documentos considerados essenciais para atingir os objetivos do estudo, isto é, documentos que contêm informações acerca das práticas de cibersegurança na organização, sobre o compromisso da instituição em assegurar a segurança da informação tanto da instituição como dos clientes, informações que permitam perceber os desafios e benefícios da certificação ISO 27001, entre outros. No âmbito do estudo, eram pretendidos para análise os relatório e contas dos anos 2011, 2012, 2013 e 2023, últimos relatórios de auditorias internas e externas, plano de resposta a incidentes, relatório de incidentes, relatório de avaliação, documentos de políticas e procedimentos internos de segurança. Contudo, tendo em conta a sensibilidade do tema e a natureza dos documentos, os documentos internos não foram facultados por serem documentos confidenciais. Com isso, foram selecionados para estudo os relatórios e contas dos anos 2011, 2012, 2013 e 2023, período antes, durante e após a certificação ISO 27001 e o presente da CECV. De acordo com Marconi e Lakatos (2003), são documentos escritos e oficiais com dados primários (produzidos pela própria CECV), cuja fonte são os arquivos particulares de instituições de ordem privada, destacando o facto de o investigador não ter influência na criação dos documentos, devendo por isso selecionar somente o material relevante e útil para o estudo.

3.5. MÉTODO DE ANÁLISE DE DADOS

Quanto à análise dos dados recolhidos, em relação às entrevistas semiestruturadas, pretende-se fazer uma análise qualitativa dos dados primários resultantes das entrevistas, uma vez que se trata essencialmente de dados não numéricos, sobre os quais pretende-se estabelecer possíveis relações entre as informações. Levando em

consideração Quivy e Campenhoudt (1998) que afirmam que as entrevistas estão sempre ligadas a um método de análise de conteúdo, optou-se por este método de análise. Para Berelson (n.d., *cit in* Bardin, 1977, pp. 34), a análise de conteúdo trata-se de "uma técnica de investigação que através de uma descrição objetiva, sistemática e quantitativa do conteúdo manifesto das comunicações, tem por finalidade a interpretação destas mesmas comunicações". Bardin (1977) refere que a análise de conteúdo potencia a capacidade exploratória, aumentando o alcance da descoberta na investigação (função heurística) e serve de meio de confirmação (função de administração da prova). De acordo com o mesmo autor, este método engloba três fases que foram seguidos ao longo desta investigação:

1) Pré-análise: consiste na organização da própria análise nomeadamente estabelecimento dos documentos sujeitos à análise e definição dos objetivos de investigação. Esta fase é caraterizada por uma leitura flutuante dos documentos por forma a extrair primeiras impressões e orientações e preparar a análise.
2) Exploração do material: esta fase destina-se essencialmente à codificação e categorização do conteúdo das entrevistas. Uma boa categorização deve seguir algumas regras, tais como a exclusão mútua (cada elemento não pode pertencer a mais de uma categoria), a homogeneidade (deve ser seguido um único princípio de classificação), a pertinência (as categorias devem ser adaptadas ao material de análise e aos objetivos da investigação), a objetividade e fidelidade (diferentes partes de um mesmo material devem ser codificadas de forma consistente) e a produtividade (as categorias devem ser produtivas, oferecendo resultados frutíferos).
3) Tratamento dos resultados obtidos e interpretação: nesta fase pretende-se fazer o tratamento dos dados por forma a validá-los e torná-los significativos, por forma a fornecer interpretações de acordo com objetivos estabelecidos inicialmente.

No caso desta investigação, as entrevistas gravadas foram transcritas e de seguida alvo de uma primeira leitura, sublinhando ideias chaves, por forma a organizar melhor as ideias sobre as informações extraídas das entrevistas e estruturar a análise dos dados. De seguida procedeu-se à codificação e categorização do conteúdo das entrevistas. A técnica de codificação permite a conversão e agregação dos dados brutos das entrevistas em unidades com caraterísticas relevantes do conteúdo (Holsi, 1969 *cit in* Bardin,

1977). Esta técnica engloba três etapas: Recorte (escolha das unidades de registo), Enumeração (escolha de regras de contagem) e Classificação e agregação (escolha das categorias). Segundo Bardin (1977), estas fases devem ser cumpridas no caso de a análise ser quantitativa e categorial e, sabendo que a análise pretendida nesta investigação é qualitativa, ignorou-se a segunda etapa de enumeração seguindo regras de contagem. Precisamente por ser uma análise qualitativa, para realizar a terceira etapa optou-se pela técnica de análise categorial. Através desta técnica, os dados foram classificados seguindo o processo de categorização que consiste em definir categorias compostas por elementos com caraterísticas comuns entre eles. Seguiu-se o critério semântico, isto é, definiu-se categorias temáticas cujos elementos agrupam-se pelo tema (Bardin, 1977).

No que diz respeito aos dados primários derivados dos questionários, considerou-se a análise quantitativa, visto que o tratamento das informações é feito de forma mais objetivo e recorrendo a métodos estatísticos, como refere Bardin (1977). Portanto, foi realizado uma análise estatística descritiva que, de acordo com Hill e Hill (2009), permite descrever resumidamente as principais caraterísticas da variável em estudo na amostra, recorrendo a medidas de tendência central como a média, mediana e a moda. Para a realização desta análise estatística descritiva, recorreu-se ao SPSS (*Statistical Package for the Social* Sciences) que se trata de um *software* informático projetado para executar cálculos estatísticos complexos e apresentar os resultados em questão de segundos, tal como define Pereira (2004). O mesmo autor chama a atenção a importância de saber que teste estatístico utilizar e de saber como interpretar de forma correta os resultados fornecidos pelo *software*. Utilizou-se a versão IBM SPSS *Statistics* 20.

Tendo em conta que os questionários, tanto dos clientes como dos funcionários, contêm perguntas abertas, também será utilizada a análise de conteúdo para a análise destas questões.

Convém referir que os dados quantitativos obtidos por meio dos questionários, mesmo que coletados a partir de amostras não estritamente representativas, servem para complementar a análise feita às entrevistas, confrontando-as com os dados das entrevistas através da triangulação de informações.

Por fim, os documentos recolhidos foram alvos de uma pequena análise documental, definida por Bardin (1977), como um conjunto de ações realizadas num documento para facilitar a sua consulta e referência, através da transformação do conteúdo original do documento para um formato diferente. Com a análise desses documentos, pretendia-se retirar o máximo de informações e conclusões relacionados com o tema e os objetivos da investigação, por forma a complementar a análise feita aos dados fornecidos pelas entrevistas e pelos questionários. Quivy e Campenhoudt (1998) consideram a análise feita a documentos uma análise secundária e mais superficial devido à limitação do investigador causado por dificuldades de compatibilidade dos dados entre si e com fenómeno a ser estudado na investigação.

3.6. QUESTÕES ÉTICAS

É reconhecida o importante papel dos participantes na investigação, nomeadamente os entrevistados, os respondentes dos questionários e a própria instituição da CECV em si, contudo é igualmente importante referir que questões éticas devem e foram levadas em conta durante a realização da investigação. Essas questões éticas são importantes por forma a garantir a integridade do estudo e o respeito dos direitos dos participantes.

Tendo em conta que a instituição é uma instituição crítica do país (o segundo maior banco nacional), o cuidado com os dados recolhidos esteve sempre presente. Com isso, durante todo a investigação reservou-se a confidencialidade, a privacidade e o anonimato dos participantes, tanto em relação às entrevistas como aos questionários. A investigação foi conduzida sempre de forma a não prejudicar a CECV e tão pouco os colaboradores.

Importante referir a existência de um acordo de confidencialidade assinado entre o investigador e a CECV, por forma a afinar os pormenores do estudo, atribuir deveres e responsabilidades, mas principalmente proteger as informações da instituição. Importante referir o dever de sigilo sobre as informações relativas à CECV.

Por se tratar de um tema sensível (segurança), algumas informações pretendidas não foram disponibilizadas, o qual compreende-se perfeitamente.

4. ESTUDO DE CASO

Este capítulo destina-se essencialmente a realização do estudo de caso, introduzido por uma breve apresentação da CECV, instituição que será o objeto do estudo. De seguida, serão aplicadas as técnicas de recolha de dados e análise dos mesmos, técnicas definidas no capítulo da metodologia. O capítulo fecha com a análise dos resultados encontrados do estudo.

4.1. APRESENTAÇÃO DA EMPRESA EM ESTUDO

Inicialmente designada por "Caixa Económica Postal", era um serviço criado em 18 de maio de 1928 integrado nos Correios e telegráficos administrado pelo Ministério das Telecomunicações. Somente em dezembro de 1985 passou a ser uma instituição financeira autónoma, sendo desde então designada Caixa Económica de Cabo Verde. A instituição preza por um serviço financeiro global de qualidade, assumindo o compromisso de ser um banco de referência nacional, sustentado pela inovação tecnológica e comercial. A CECV é atualmente o segundo maior banco nacional em termos de volume de negócios, sendo destacado como líder em termos de transformação digital em Cabo Verde pelo último Relatório e Contas (CECV, 2023). A CECV é até ao momento o único banco de Cabo Verde certificado internacionalmente pela ISO 27001:2013 e ISO 9001:2015, em relação ao Sistema de Gestão da Segurança de Informação e ao Sistema de Gestão da Qualidade, respetivamente.

Atualmente, o capital social da CECV é de 1.392.000.000 escudos (CVE), sendo que até 2023 o Estado de Cabo Verde, através do Ministério das Finanças, detinha 27,44% das ações da instituição, mas foram vendidas na Bolsa de Valores de Cabo Verde no início de 2024. Assim, a estrutura acionista atual da CECV tem a seguinte composição:

Tabela 1: Estrutura Acionista da CECV

Entidade	Nº de Ações	Percentagem
Instituto Nacional de Previdência Social (INPS)	657 200	47,21%
Correios de Cabo Verde	210 749	15,14%
Outros subscritores e trabalhadores	524 051	37,65%
Total	1 392 000	100%

***Fonte**: https://www.caixa.cv/institution*

De acordo com o último relatório e contas da instituição, a CECV detém uma quota de mercado em termos de volume de negócio de 31,59% graças às 33 agências e 7 delegações espalhadas por todo o território nacional. Até ao final de 2023, a instituição empregava um total de 376 colaboradores e contava com uma carteira com mais de 336.000 clientes, entre particulares e empresas (CECV, 2023).

Com um objetivo muito claro em manter a sustentabilidade da rendibilidade, eficiência e solidez financeira, a instituição tem vindo a proporcionar resultados satisfatórios para os *stakeholders*, apresentando um resultado e rendimento integral de 1.503.179 milhares de escudos no último exercício. Deste resultado, o Conselho de Administração propôs-se a distribuir 50% em dividendos. Graças a esses resultados, a instituição apresentou excelentes indicadores de rentabilidade: Retorno sobre o Ativo de 1,71 (ROA, em inglês *Return on Assets*); Rendibilidade dos Capitais Próprios de 18,91 (ROE, em inglês *Return on Equity*). Além desses indicadores, a CECV apresentou um rácio de solvabilidade de 24,63%, considerado um excelente indicador de risco financeiro (CECV, 2023).

4.2. APLICAÇÃO DE TÉCNICAS DE RECOLHA E TRATAMENTO DE DADOS

4.2.1. Entrevistas

Conforme definido na metodologia, foram realizadas duas entrevistas, ambas semiestruturadas: uma (designada ao longo do estudo por **E1**) com um colaborador da área de Comunicação, Informática e Segurança (**I1**); e outra (designada ao longo do estudo por **E2**) com dois profissionais Administradores de Rede da CECV (**I2** e **I3**). Ambas as entrevistas foram realizadas online através da plataforma Zoom, visto que estes profissionais se encontram em Cabo Verde e aproveitou-se as vantagens que a digitalização e a conetividade nos oferecem. Nas duas entrevistas foi solicitada e prontamente aceite pelos entrevistados, a gravação em áudio e vídeo das mesmas, garantindo a confidencialidade e o uso das informações exclusivamente para fins académicos.

O guião da E1 (Apêndice A) contou com um total de 27 perguntas divididas em 10 blocos sobre a história e atualidade da CECV, as principais estratégias e políticas de

mitigação de riscos cibernéticos, os impactos da ISO 27001, os desafios e as principais tecnologias e investimentos realizados pela CECV no âmbito da cibersegurança. Todas as questões foram respondidas ao longo da entrevista, sem ser por ordem do guião, tal como define as entrevistas semiestruturadas. No início da entrevista, apresentou-se o investigador de forma rápida e bem como a investigação e os seus objetivos. A entrevista E1 teve uma duração de aproximadamente 50 minutos, pelo que no final agradeceu-se ao entrevistado pela disponibilidade em fornecer informações muito valiosas para a investigação.

A E2 compreendeu um total de 18 perguntas distribuídas por 10 blocos (conforme Apêndice B) com tópicos relativos ao contexto pessoal dos entrevistados, a infraestrutura de rede e políticas de segurança, formação dentro da CECV, a certificação ISO 27001, os principais desafios as e principais ferramentas de combate às ameaças cibernéticas da CECV. Destas 18 questões, 2 não foram respondidas: uma por motivos de confidencialidade de informações e outra por estar fora do âmbito das suas funções. Uma 3ª questão foi preterida pelo investigador ao longo da entrevista por gestão de tempo, visto que essa questão fora respondida na entrevista E1 e o tempo dos entrevistados era limitado. Tal como aconteceu na entrevista E1, começou-se a entrevista E2 com uma pequena apresentação do investigador e da investigação e seus objetivos por forma a contextualizar os entrevistados com o assunto. A entrevista E2 teve uma duração de aproximadamente 36 minutos, finalizada pelos agradecimentos aos entrevistados pela disponibilidade e valiosa contribuição no estudo. De acrescentar que um dos profissionais entrevistados (I2) chegou minutos atrasados e faltou as duas primeiras questões, mas por serem introdutórias e o tempo limitado decidiu-se avançar com a entrevista.

Após a realização das entrevistas, ambas foram transcritas com o apoio das gravações para uma melhor análise dos dados, conforme em Apêndice C e D. Seguiu-se a análise de conteúdo através das três fases enunciadas no capítulo anterior. O processo de análise de conteúdo das entrevistas foi realizado individualmente, completando todas as etapas para uma entrevista antes de iniciar a análise da próxima. Analisou-se a E1 primeiro por ser mais extensa e conter informações que facilitaram a análise subsequente da E2.

A primeira fase, designada Pré-Análise, destinou-se à realização da leitura flutuante às entrevistas (E1 e E2), sublinhando às ideias chaves e organizando a própria análise feita na fase a seguir.

Seguiu-se a segunda fase, a exploração do material. Seguindo os procedimentos descritos anteriormente, construiu-se os seguintes quadros (Quadro 2 e Quadro 3) com as categorias e subcategorias para o tratamento do conteúdo das entrevistas E1 e E2, tendo em conta as regras de categorização enunciadas no capítulo anterior.

Quadro 2: Categorias e Subcategorias E1

Categorias	Subcategorias
A. Contexto do mercado cabo-verdiano	A.1 Posicionamento no mercado interbancário de Cabo Verde A.2 Cibersegurança no contexto nacional
B. Estratégias de Cibersegurança	B.1 Infraestruturas, tecnologias e ferramentas existentes B.2 Procedimentos de resposta e de proteção dos dados e produtos/serviços B.3 Políticas e normativos internos B.4 Histórico de incidentes cibernéticos
C. Certificação ISO 27001	C.1 Principais benefícios e implicações resultantes da certificação ISO 27001 C.2 Custos, desafios e duração do processo de obtenção da certificação
D. Cultura Organizacional e Capacitação	D.1 Existência de ações de formação, sensibilização e desenvolvimento em matéria de cibersegurança D.2 Principais investimentos em cibersegurança D.3 Principais vulnerabilidades, desafios e ameaças à instituição D.4 Desafios trazidos pela Covid-19 e processo da digitalização D.5 Feedbacks e oportunidades de melhoria

Quadro 3: Categorias e Subcategorias E2

Categorias	Subcategorias
A. Perfil do Entrevistado	A.1 Percurso acadêmico A.2 Experiência profissional e funções atuais
B. Infraestrutura de Rede e Tecnologias de Segurança	B.1 Descrição da infraestrutura de rede da instituição B.2 Tecnologias e Ferramentas de Segurança
C. Processos e Procedimentos	C.1 Procedimentos, medidas e políticas de proteção de sistemas e dados C.2 Principais benefícios e implicações resultantes da certificação ISO 27001
D. Cultura Organizacional e Capacitação em Segurança	D.1 Existência de ações de formação, sensibilização e desenvolvimento em matéria de cibersegurança D.2 Principais vulnerabilidades, desafios e ameaças à instituição D.3 Áreas e oportunidades de melhoria

Após definir-se as categorias e subcategorias de análise para cada uma das entrevistas, realizou-se a análise de conteúdo das duas entrevistas através da construção de quadros levando em conta as categorias, subcategorias e unidades de registo. Por serem quadros extensos e para melhor organizar os dados no documento, os quadros preenchidos encontram-se em anexo (Apêndice E e F), sendo que a estrutura base dos quadros é a que se apresenta abaixo no Quadro 4:

Quadro 4: Estrutura base dos quadros de análise de conteúdo

Categorias	
Subcategorias	**Unidades de Registo**

4.2.2. Questionários

Como já referido no capítulo referente à metodologia, para a recolha de dados foram aplicados dois questionários: um destinado a colaboradores da CECV (designada ao

longo do estudo por Q1) e outro a clientes da mesma instituição (designada ao longo do estudo por Q2). Ambos os questionários foram construídos, disponibilizados e preenchidos de forma online, através da plataforma *Google Forms* e posteriormente tratados no *software SPSS*.

A recolha dos dados através dos questionários iniciou-se na segunda metade de julho e foram encerradas na segunda metade de agosto, portanto, os inquiridos tiveram sensivelmente 1 mês para responder aos questionários. Após a receção das respostas através da plataforma Google *Forms*, estas foram extraídas para uma folha do Excel, onde foram tratadas e codificadas por forma a serem introduzidas, de seguida, no *software* estatístico SPSS para o tratamento dos dados.

O questionário aplicado aos colaboradores (Q1) encontra-se em anexo (Apêndice G) e contou com 22 questões, sendo 18 delas fechadas e 4 abertas. Além de uma primeira secção de apresentação e introdução ao questionário, estas questões estavam enquadradas em outras 6 secções: dados de identificação; conhecimento e formação; perceção sobre riscos cibernéticos; eficácia das estratégias de mitigação; melhorias e sugestões; e *feedback* geral. O questionário foi distribuído internamente, de forma massiva, aos colaboradores da CECV pelo responsável de comunicação da instituição. Sendo conhecida a fraca aderência dos colaboradores a questionários e inquéritos e apesar dos esforços para incentivar a resposta ao questionário, a amostra final consistiu em apenas 15 respostas.

Em relação ao género, dos 15 inquiridos, 6 são do sexo masculino (40%) e cerca de 9 são do sexo feminino (60%), constituindo a maioria da amostra. A distribuição segue representada na Figura 1 a seguir:

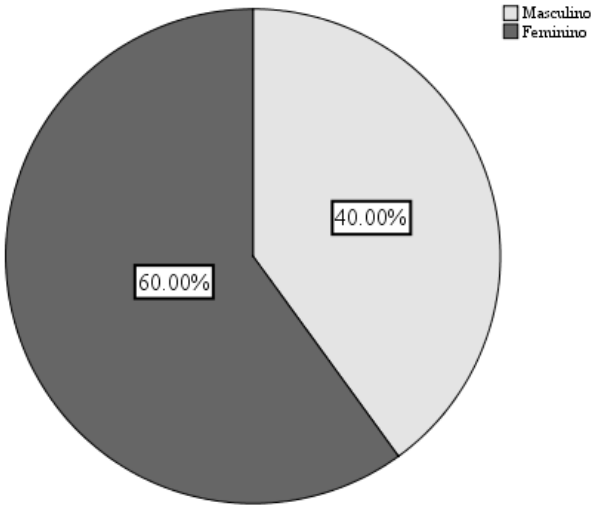

Figura 1: Distribuição por gênero (funcionários)

Quanto à idade, a idade média dos inquiridos é de aproximadamente 47 anos, sendo 37 anos a idade mínima e 58 anos a idade máxima. Estes números aproximam da realidade da instituição em que a idade média dos colaboradores é de 44 anos, de acordo com os dados do último Relatório e Contas (CECV, 2023). Representando a amostra por faixas etárias, cerca de 26,7% dos inquiridos têm idade compreendida entre os 30 e 40 anos, 40% entre os 41 e 50 anos, e 33,3% de 51 a 60 anos, como se apresenta na Figura 2:

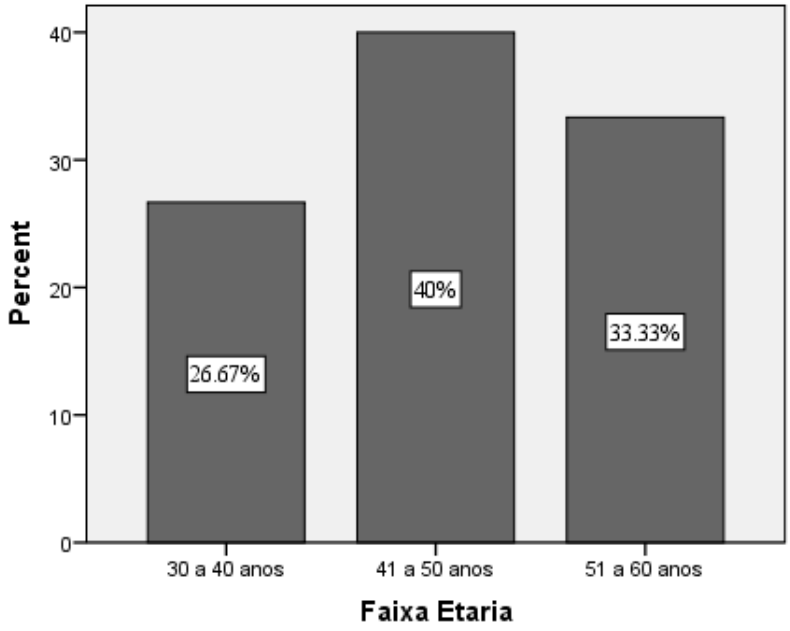

Figura 2: Distribuição por faixa etária (funcionários)

No que toca ao nível de escolaridade, todos os funcionários que responderam ao questionário têm completado o ensino superior.

Quanto ao departamento de serviço na CECV, os inquiridos encontram-se distribuídos por 7 departamentos diferentes. *Compliance* é o departamento mais representado com cerca de 26,67% dos inquiridos, seguido do Administrativo com 20%. Os departamentos Financeiro, Operacional e Risco cada um equivale a 13,33% dos inquiridos. Tanto o departamento Comercial como o de Avaliação Imobiliária, cada um representa igualmente 6,67% dos inquiridos. (Tabela 2)

Tabela 2: Distribuição por departamentos

	Frequência	**Percentagem**	**%Acumulada**
Compliance	4	26,67%	26,67%
Administrativo	3	20%	46,67%
Financeiro	2	13,33%	60%
Operacional	2	13,33%	73,33%
Risco	2	13,33%	86,66%
Avaliação Imobiliária	1	6,67%	93,33%
Comercial	1	6,67%	100%
Total	15	100%	

Em relação ao tempo de serviço dos inquiridos na CECV, os funcionários inquiridos estão, em média, aproximadamente há 18 anos na instituição. O inquirido mais recente está na CECV há 5 anos, sendo que o mais antigo está há 29 anos. Representando a amostra através de categorias consoante a antiguidade, 3 inquiridos estão na CECV há 5 anos ou menos, nenhum está entre 6 a 10 anos, 4 estão na instituição entre 11 a 20 anos e a maior parte (8) está há mais de 20 anos na CECV. Essa distribuição está representada a seguir na Figura 3:

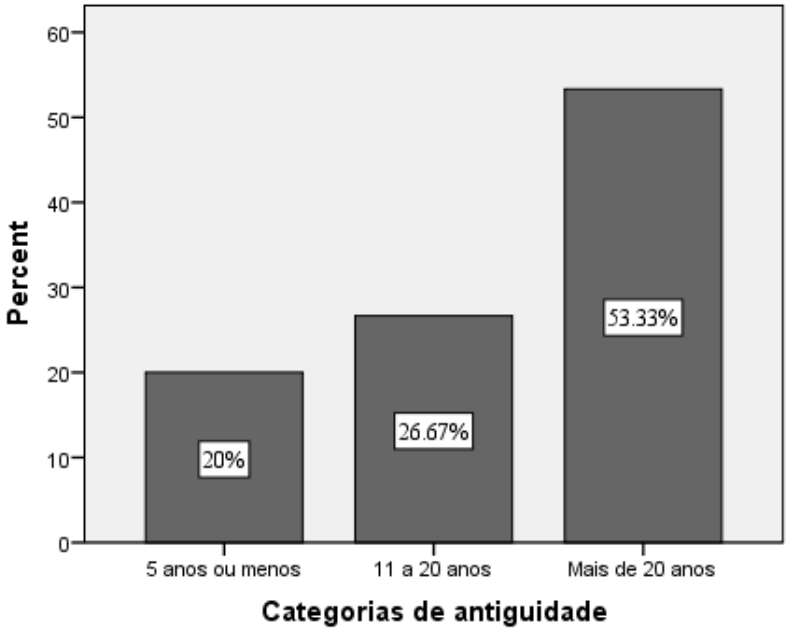

Figura 3: Distribuição por categorias de antiguidade

Para a análise das perguntas abertas, 2 foram codificadas e analisadas quantitativamente através do *software*. Não foram fornecidas sugestões, com isso não há conteúdo a ser analisada na pergunta destinada a sugestões. Sendo assim, apenas a questão relacionada com comentários foi alvo de uma pequena análise de conteúdo (apenas 4 comentários) feita através de uma grelha composta por categoria, subcategorias e unidades de registo apresentada a seguir (Quadro 5). De referir que para tratamento dos dados os inquiridos foram designados de FI (Funcionário Inquirido).

Quadro 5: Análise de conteúdo de pergunta aberta do Q1

Categoria: Sugestões/Comentários	
Subcategoria	**Unidades de Registo**
Importância de cibersegurança	(FI 3) "A cibersegurança é importante para a CECV (…) caraterizado como banco sistémico no sistema financeiro de Cabo Verde" (FI 3) "Dados são importantes uma vez que envolve informações de terceiros" (FI 7) "Alerta máxima, ninguém está imune"
Políticas e boas práticas	**(**FI 12) "Reforçar as medidas preventivas" (FI 15) "Contrariamente às boas práticas internacionais, a Direção de Informática, Comunicação e Segurança é responsável simultaneamente pela Informática e Segurança Informática"

Quanto ao questionário destinado a clientes (Q2), em anexo (Apêndice H), foi constituída por 6 secções: apresentação e introdução ao questionário; dados de identificação; utilização de serviços online; perceção de segurança e experiência com incidentes cibernéticos; conhecimento e formação; e *feedback* e sugestões. Ao longo destas secções foram distribuídas 20 questões, sendo 16 fechadas e 4 abertas. Distribuído pelo próprio investigador através de um link para o Google Forms, o Q2 foi divulgado essencialmente através de redes sociais (Facebook e Instagram) e através de contactos diretos com inquiridos conhecidos que fossem clientes da CECV. De referir que, de uma forma geral, os alvos alcançados pelo pedido mostraram recetivos a participar no estudo. Com isso, resultou numa amostra final de 79 respostas de clientes da CECV, particulares e empresas.

Em relação à tipologia de cliente, a amostra final é constituída por uma maioria esmagadora de clientes particulares. Cerca de 97,5% da amostra são clientes particulares da CECV (77 indivíduos), sendo que apenas 2 empresas responderam ao questionário, representando 2,5% da amostra (Figura 4). A fraca adesão de empresas ao estudo deve-se sobretudo ao poder de alcance às empresas por parte do investigador, uma vez que não foi possível a distribuição do questionário aos clientes CECV através da própria CECV, como explicado anteriormente no capítulo destinado à metodologia.

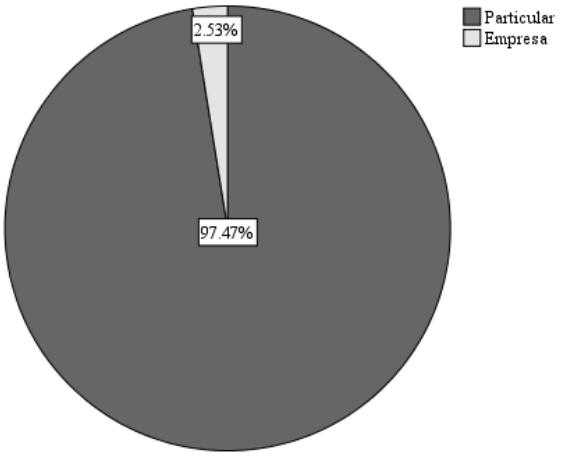

Figura 4: Distribuição por tipologia de cliente

Quanto à distribuição dos clientes particulares por género, cerca de 44,2% são do sexo masculino, totalizando 34 indivíduos, enquanto 55,8% são mulheres, correspondendo a 43 pessoas. Vale mencionar que pelo facto de existirem 2 empresas na amostra, estas naturalmente não entram na distribuição por género e por isso são considerados pelo *software* estatístico como *missing values*, como se apresenta na Figura 5 seguinte:

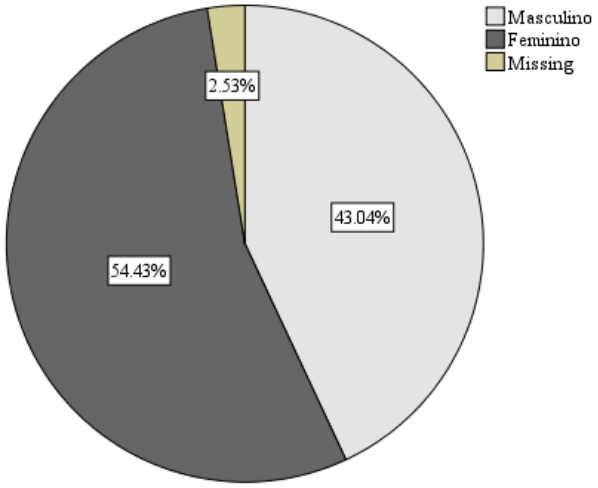

Figura 5: Distribuição por género (particulares)

No que toca a idade dos clientes particulares, a idade média dos inquiridos é de aproximadamente 30 anos, sendo 18 anos a idade mínima e 60 anos a idade da pessoa mais velha. Analisando por faixa etária, apenas 2 indivíduos possuem menos de 20

anos, a maioria (53) com idade dos 20 aos 30 anos, 13 inquiridos com idade compreendida entre 31 e 40 anos, apenas 3 indivíduos entre 41 e 50 anos e 5 com mais de 50 anos, o que demostra alguma variedade de clientes de praticamente todas as faixas etárias, representadas na Figura 6:

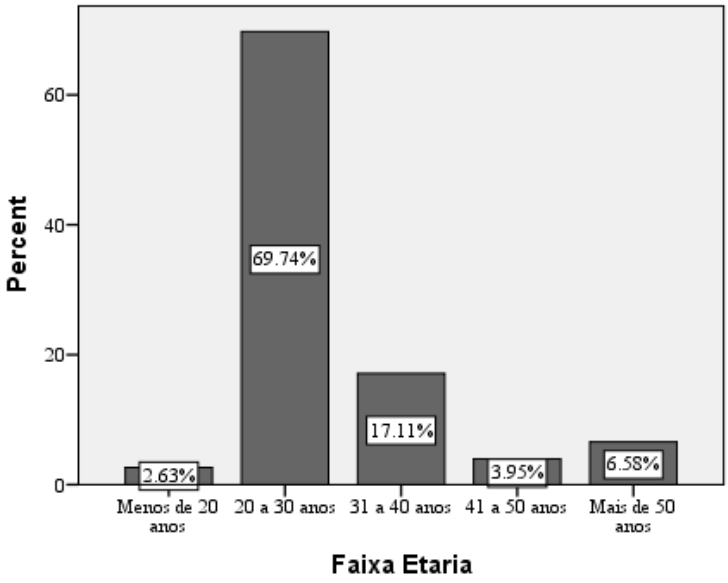

Figura 6: Distribuição por faixa etária (particulares)

Quanto ao nível de escolaridade, a amostra possui apenas clientes particulares pertencentes ao Ensino Secundário e ao Ensino Superior. A maioria enquadra-se no Ensino Superior, cerca de 64 indivíduos, o que equivale a 83,1% da amostra. Os restantes 16,9% correspondentes a 13 indivíduos, possuem o Ensino Secundário (Figura 7).

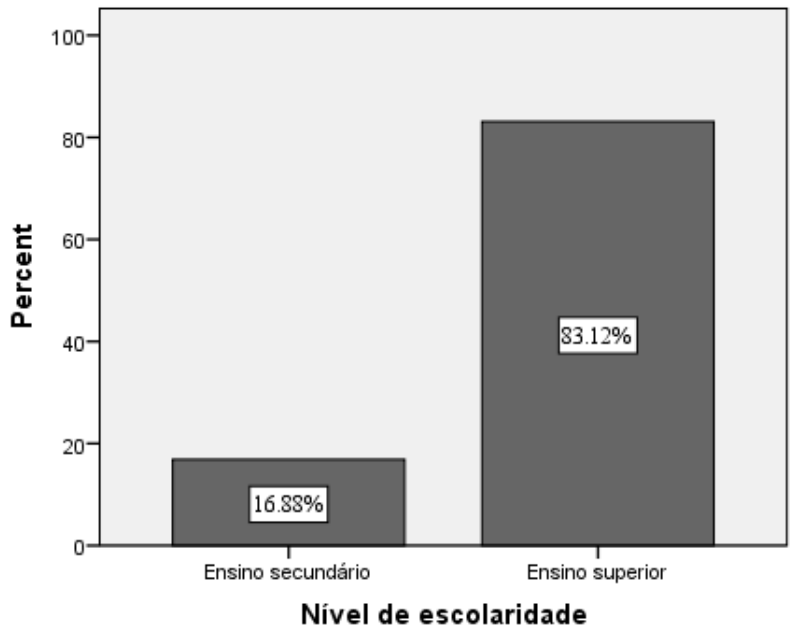

Figura 7: Distribuição por nível de escolaridade (particulares)

Em relação à antiguidade dos inquiridos como clientes (empresas e particulares) da CECV, verifica-se que, em média, os inquiridos são clientes da CECV há aproximadamente 10 anos, sendo o inquirido cliente mais antigo pertencente à instituição há 32 anos. Existem cerca de 6 inquiridos clientes da CECV há 1 ano ou menos. Analisando os inquiridos por categorias de antiguidade (Figura 8), pode-se constatar que existem igualmente clientes da CECV há 5 anos ou menos e entre 6 a 10 anos, cada categoria com 26 clientes. Cerca de 13 inquiridos são clientes da CECV entre 11 a 20 anos e apenas 9 há mais de 20 anos. Esta questão contou com 5 respostas inválidas, não consideradas pelo *software*.

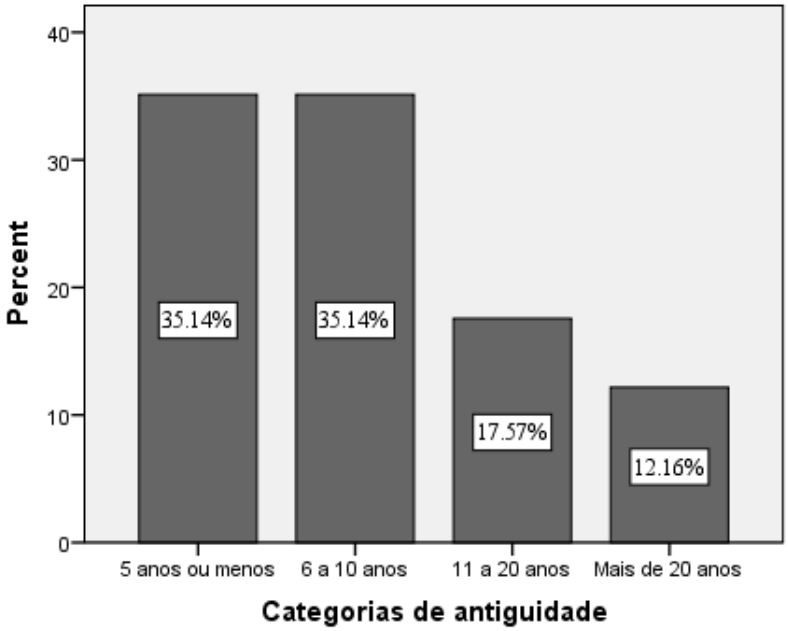

Figura 8: Distribuição por antiguidade (clientes)

Quanto ao tratamento das perguntas abertas, 2 das 4 perguntas foram codificadas e tratadas quantitativamente através do *software*. Uma outra relacionada com a descrição de algum ataque cibernético a que foi alvo, só houve uma única resposta. Em relação à questão destinada a sugestões e comentários, realizou-se uma pequena análise de conteúdo, semelhante a realizada para o Q1. Foi feita através de uma grelha composta por categoria, subcategoria e unidades de registo apresentada a seguir (Quadro 6). De referir que para tratamento dos dados os inquiridos foram designados de CI (Cliente Inquirido).

Quadro 6: Análise de conteúdo de pergunta aberta do Q2

Categoria: Sugestões/Comentários	
Subcategoria	**Unidades de Registo**
Melhorias em produtos e serviços	(CI 9) "Aumentar o número de dígitos para escolha da chave de confirmação." (CI 13) "Em vez de enviar o código de confirmação para telemóvel (…) o enviassem para email" (CI 15) "Satisfeito" (CI 30) "Melhorar a plataforma" (CI 52) "Melhorar o aplicativo da CaixaNet" (CI 54) "CaixaNet é muito instável, sem sempre consigo ter acesso." (CI 74) "Depois do horário de funcionamento, algumas funcionalidades deixam de dar resposta"

4.2.3. Documentos

Com o objetivo de proporcionar a triangulação de informações, como mencionado na metodologia, foram analisados os Relatório e Contas da CECV dos anos 2011, 2012, 2013 e 2023. Todos os relatórios foram recolhidos do site do Banco Central de Cabo Verde.

Para a análise, os relatórios foram alvo de leituras por forma a retirar informações relevantes para o estudo. Por forma a organizar os dados para melhor consulta, construiu-se um quadro resumo com as principais informações extraídas. O quadro encontra-se em anexo (Apêndice I).

4.3. ANÁLISE DOS RESULTADOS

Relembrando que os objetivos do estudo são a avaliação da eficácia das estratégias de mitigação de riscos cibernéticos na CECV, identificação de custos, desafios e benefícios da certificação ISO 27001 e a identificação de vulnerabilidades e sugestão de melhorias para a instituição, segue-se a análise dos resultados.

Considerando os métodos utilizados na recolha e tratamento de dados, para melhor estruturar a apresentação dos resultados, a análise será feita de acordo com as categorias

definidas no Anexo A da ISO 27001: Organizacional, Pessoas, Físico e Tecnologia. A essas categorias, acrescenta-se duas outras relacionadas com a Certificação ISO 27001 e com as Preocupações, Ameaças e Sugestões.

4.3.1. Organizacional

Esta categoria visa essencialmente avaliar as políticas, os procedimentos e medidas de controlo que a CECV, enquanto organização, tem adotado para mitigar os riscos cibernéticos e garantir a segurança da informação.

Começando pelos procedimentos de cibersegurança existentes na instituição, destaca-se desde logo a existência de múltiplas auditorias na CECV, tanto internas como externas. Existe um "processo de auditorias regulares em que são realizadas 4 auditorias internas e 2 auditorias externas…" (I1) além da entidade certificadora da ISO 27001, Bureau Veritas, que "uma vez por ano…faz o processo de acompanhamento de como tem sido o tratamento da segurança da informação" (I1). Convém referir que as auditorias internas anuais, realizadas em conjunto com um "parceiro de cibersegurança" (I3), têm a principal função de "preparar a instituição para auditorias formais do emissor do certificado" (I3). Nota-se então a existência de um "gabinete interno de auditorias de sistemas de informação da CECV" (I2). Também, o serviço *mobile banking* CaixaNet e o portal da CECV são alvos de "monitorização e auditorias regulares de *pentest*", isto é, testes de penetração.

Todos esses processos de auditoria são importantes para a instituição uma vez que "a visão do auditor…permite executar tarefas de acordo com as boas práticas" (I1) graças aos relatórios de *findings* produzidos e que "são categorizados como oportunidades de melhoria, observação ou não conformidade (menor ou maior)" (I1). Além de um sinal bastante positivo deixado pelas auditorias, visto que até agora "nunca a instituição teve uma não conformidade maior" (I1), estas "permitem sempre melhorar a instituição" (I1) uma vez que a instituição recorre a "consultores externos e técnicos internos para lidar com as sugestões dos auditores" (I1).

Outro aspeto importante nas estratégias de mitigação de riscos cibernéticos passa pela existência de normativos e documentos sobre a segurança da informação. De acordo com os dados do Relatório e Contas de 2013, a CECV, desde 2013, elaborou o manual de segurança, plano de segurança e o plano de emergência e evacuações. Atualmente a

instituição possui "4 tipos de documentos: normas, manuais, procedimentos e registos." (I1). Esses documentos são "geridos, aprovados e revistos anualmente por uma comissão de segurança formada pelos administradores executivos, pelo auditor interno, pela direção de informática, por auditores externos e por consultores externos" (I1). Após serem aprovados, "os documentos são disponibilizados na *intranet* da instituição para todos os colaboradores terem acesso" (I1). A instituição possui de forma documentada, um "plano de continuidade de negócio" e um "plano de recuperação de desastres" (I1). A eficiência desses planos é testada "duas vez por ano" através de uma "simulação de catástrofe no *data center* da instituição" (I1), visto que "a CECV nunca teve uma situação real e de grande dimensão que necessitasse a ativação dos planos" (I1). Em relação aos dados obtidos do questionário aplicado aos colaboradores (Tabela 3), 20% afirmam que a CECV nunca sofreu um ataque cibernético significativo e 73,3% assumem que não sabem se a instituição já foi alguma vez alvo de um ataque significativo, o que poderá ser interpretada como um sinal de que a instituição nunca ter sido atacada de forma significativa, pois os efeitos seriam sempre bastante visíveis.

Tabela 3: Conhecimento dos colaboradores sobre ataques cibernéticos na CECV

	Frequency	Percent	Valid Percent	Cumulative Percent
Sim	1	6.7	6.7	6.7
Não	3	20.0	20.0	26.7
Não sei	11	73.3	73.3	100.0
Total	15	100.0	100.0	

Contudo, apesar da instituição nunca ter sido alvo de um ataque cibernético de alguma dimensão, funcionários no desempenho das suas funções já foram alvo de tentativas de ataques cibernéticos como é cada vez mais frequente. 35,3% dos colaboradores já foram alvo de alguma engenharia social, enquanto 29,4% dos colaboradores admitem já terem sido visados por ataques *malware* (Tabela 4). Quanto aos clientes (Tabela 5), 87,3% dos inquiridos afirmam que nunca foram alvo de ataques cibernéticos, enquanto 11,4% não sabem se já foram ou não atacados. De referir que no passado, "já houve casos de ataques *phishing* com clientes a serem afetados na *internet banking"* (I1), situação que foi resolvida através da implementação do *one-time password.*

Tabela 4: Colaboradores alvos de tentativas de ataques cibernéticos

Ataques Cibernéticos	N	Percent
Engenharia Social	6	35.3%
Malware	5	29.4%
Ransomware	1	5.9%
Nenhuma	5	29.4%
	17	100.0%

Tabela 5: Clientes alvo de ataques cibernéticos

	Frequency	Percent	Valid Percent	Cumulative Percent
Sim	1	1.3	1.3	1.3
Não	69	87.3	87.3	88.6
Não Sei	9	11.4	11.4	100.0
Total	79	100.0	100.0	

Em relação aos procedimentos de controlo de acesso e identidade na CECV, existe uma série de ações por forma a salvaguardar o acesso à instituição. A instituição encontra-se equipada com "servidores de gestão de acessos e identidades" (I3), sendo o *data center* protegido com sistema "controlo biométrico que regista as entradas (quem e quando teve acesso) e controla quem pode ter acesso" (I3), além dos "controlos climáticos, portanto, temperatura, humidade e ar condicionado" (I3). Quanto ao acesso de colaboradores, enquanto utilizadores, são alvo de controlos apertados nas contas principalmente em relação às *passwords* que devem ser "alteradas, … com um mínimo de carateres, incluindo carateres especiais, complexos" (I3). Dos colaboradores, destacam-se os administradores de infraestruturas que são alvos de "controlos mais apertados e restritos em relação ao tempo de vida das *passwords*, seu tamanho e sua complexidade… uma vez que têm acessos mais privilegiados" (I3). Convém mencionar que "todos os registos e *logins* dos utilizadores são gravados para consulta posterior" (I3) caso for necessário. Também a CECV tem implementada uma política de "bloqueio a qualquer acesso de qualquer colaborador do banco que esteja fora de Cabo Verde" (I1) sem que este tenha avisado antecipadamente o departamento de Informática. Recentemente, a instituição iniciou o processo "*multifactor authenticator* para os

colaboradores" (I1) por forma a garantir maior controlo e segurança no acesso dos mesmos.

Quanto à monitorização, a CECV possui "sistema de monitorização de vídeo, acompanhada 24h/dia pela equipa de segurança física" (I3) que "monitoriza tudo o que seja videovigilância, intrusão, incêndio e controlo de acesso" (I1). Em caso de "qualquer alarme detetado, é comunicado ao responsável de segurança da CECV que desencadeia o processo de resolução adequado" (I1). Também o próprio sistema de *logs* "monitoriza e armazena os *logs*, regista e reporta tentativas de acesso" (I1). Qualquer alarme detetada é "monitorizada pelo departamento de segurança, informática e comunicação que faz as devidas correções" (I1). Para além das ferramentas de monitorização de acesso descritos, todas as redes das agências da CECV possuem ferramentas de monitorização de "conetividade, o CPU, a temperatura, humidade, etc." (I1). De realçar que a CECV, desde 2012, tem apostado na implementação de sistemas de monitorização de sistemas críticos, tal como destaca no Relatório e Contas referente ao exercício de 2012.

No âmbito da proteção de dados e informações, a instituição tem adotado um conjunto de outros procedimentos. Por exemplo, no Relatório e Contas 2013, é referido a implementação de segurança eletrónica nos arquivos existentes em São Vicente. Também, a CECV tem implementado políticas de não impressão, isto é, "evitar o máximo possível as impressões" (I1) uma vez que para além de se reduzir custos, reduz também o risco de vazamento de informações e dados confidencias. Neste mesmo sentido, a instituição tem "disponibilizado destruidores de papel em todas as salas" (I1), tem apostado no desenvolvimento interno de soluções digitais levando em conta a cibersegurança como a DigitalDocs (desmaterialização de atividades em papel, reduzindo o consumo em mais de 90.000 folhas de papel por ano), validação de documentos online e a SmartBot, como destaca o último Relatório e Contas 2023.

De notar que a instituição "não tem nenhuma ligação com a rede do Estado, nem com nenhuma entidade local em termos de parceria" (I1), um requisito importante na partilha de informação e cooperação entre instituições privadas, mas também com instituições públicas. As conexões existentes com outros bancos têm haver com a "partilha de uma única conetividade à rede SWIFT, através da SISP" (I1), o que representa um grande risco sistémico, e a "conetividade com o banco central" (I1). O

que traduz a falta de "colaboração entre as instituições financeiras" (I1) pela ausência de "partilha e troca de informações" (I1).

4.3.2. Pessoas

Nesta categoria, é feita a análise sobre as estratégias de mitigação de riscos de cibernéticos, tendo como foco os colaboradores, mas também os clientes.

Atualmente com 364 colaboradores ativos, sendo a maioria feminino (61% do sexo feminino, 39% do sexo masculino), a CECV conta com um recurso humano qualificado: cerca de 69% dos colaboradores têm formação superior. Dado este confirmado pelos dados obtidos do questionário em que 100% dos colaboradores inquiridos possuíam o ensino superior. Com uma idade média de 44 anos (Relatório e Contas 2023), os colaboradores inquiridos têm em média 18 anos de serviço na CECV, o que mostra alguma continuidade na instituição e um sinal de satisfação dos colaboradores. De acordo com dados do último Relatório e Contas 2023, a área comercial concentra a maior parte dos colaboradores, cerca de 63%. Já os dados dos questionários aplicados, apontam para o departamento de *Compliance*, com cerca de 26,7% dos inquiridos.

Tendo em conta o importante papel dos colaboradores nas estratégias de cibersegurança da CECV, uma vez que "qualquer colaborador é sempre um vetor de possível ataque" (I1), 66,7% dos colaboradores inquiridos admitem que o recurso humano seja o ativo mais vulnerável para a entrada de ciberataques na CECV. Neste sentido, várias são as ações da CECV no sentindo de promover a cibersegurança no ceio do seu RH, sendo uma delas a "mudança da mentalidade das pessoas" (I1). Começando desde o momento em que um colaborador novo entra na instituição onde é inserido num "processo chamado formação de integração (…) em que é dado a conhecer os normativos, o funcionamento da instituição, etc. Há uma sessão destinada a segurança de informação" (I1). Há 1 ano iniciou-se sessões online, 2 vezes por ano, do responsável de segurança na CECV para com os colaboradores "sobre temas relacionados com a segurança de informação" (I1). Ainda no seio da instituição, "existe um programa denominado Comunica Comigo, transmitido através de um canal interno no *Outlook* que aborda semanalmente um tema, incluindo boas práticas de cibersegurança, com foco no *phishing* e *ransomware*" (I1).

Um aspeto importante em relação aos colaboradores no que toca às estratégias de mitigação de riscos cibernéticos, tem haver com a formação, consciencialização e sensibilização dos funcionários sobre temas relacionados com a cibersegurança. A CECV tem mostrado ser uma instituição que investe fortemente na formação interna e externa dos seus colaboradores, de acordo com todos os relatórios e contas analisados, sendo que em 2013: 2 colaboradores foram contemplados com a formação ISO 27001 Foundation; em 2012: 6 colaboradores estiveram em formação de segurança da infraestrutura tecnológica (método "on-the-job"); em 2013: foram formados 11 colaboradores em auditoria interna; em 2023: formação dos técnicos de segurança eletrónica. Contudo, dados recolhidos dos questionários e das entrevistas apresentam tendências um pouco distintas. Apesar de 60% dos colaboradores inquiridos afirmam já ter recebido alguma formação ou iniciativa de sensibilização em matéria de cibersegurança na CECV, cerca de 40% dos colaboradores afirmam não ter recebido, o que representa um número considerável. Dos que dizem já terem recebido formações, 44% afirmam que recebem formações e ações de sensibilização pelo menos anualmente e 22% afirmam que essas ações acontecem pelo menos trimestralmente (Tabela 6). Esses dados vão de encontro com informações dos entrevistados que afirmam que "normalmente não recebem formações com periodicidade fixa (…), mas que basicamente todos os anos acontecem essas formações" (I2). Para complementar essa periodicidade, os colaboradores procuram estar "sempre informados e acompanhando as tendências" (I2), mas também através de "muita troca de informações e pequenas formações com empresa parceira" (I2) (Ver tabela 6).

Tabela 6: Frequência de formação e ações de sensibilização

Frequência de formação na CECV	**Formação/Capacitação na CECV**				**Total**
	Sim		Não		
Anualmente	4	44,4%	0	0%	4
Trimestralmente	2	22,2%	0	0%	2
Nunca	3	33,3%	6	100%	9
Total	9	100%	6	100%	15

Quanto ao nível de satisfação (Tabela 7), 33,3% dos colaboradores inquiridos mostraram-se satisfeitos com as formações e ações de sensibilização, 40% foram

neutros, sendo que 13,3% dizem estar muito insatisfeitos, como tratado na tabela 7 seguinte:

Tabela 7: Satisfação com as formações e ações de sensibilização

	Frequency	Percent	Valid Percent	Cumulative Percent
Muito satisfeito(a)	1	6,7	6,7	6,7
Satisfeito(a)	5	33,3	33,3	40,0
Neutro(a)	6	40,0	40,0	80,0
Insatisfeito(a)	1	6,7	6,7	86,7
Muito insatisfeito(a)	2	13,3	13,3	100,0
Total	15	100,0	100,0	

Nota-se um bom nível de conhecimento dos colaboradores em relação a ataques cibernéticos. A Engenharia Social (*Phishing/Smishing/Vishing*) foi o tipo de ciberataque mais conhecido pelos colaboradores inquiridos, cerca de 35,9%. Seguiu-se o *Malware* e o *Ransomware* igualmente com 25,6% de inquiridos cada (Tabela 8).

Tabela 8: Conhecimento dos colaboradores sobre ataques cibernéticos

Conhecimento de ataques	Response	
	N	Percent
Engenharia Social	14	35,9%
Malware	10	25,6%
Ransomware	10	25,6%
DDoS	5	12,8%
Total	39	100,0%

Tendo em conta que um dos objetivos das estratégias da CECV passa por salvaguardar os dados e informações não só da instituição, mas também dos clientes, é igualmente importante que a instituição esteja comprometida com a sensibilização dos clientes quanto aos riscos cibernéticos. A CECV, de acordo com o último Relatório e Contas 2023, conta com 336.163 clientes, sendo 95% destes clientes particulares. Reforçando o estatuto de pioneiro na transformação digital no mercado, a instituição tem 88.647 clientes digitais.

A CECV, no âmbito dos clientes, faz "publicações sobre alertas, cuidados e boas práticas de cibersegurança nos canais da instituição (*site*, *Facebook* e *Youtube*), mas

também por email" (I1). Dos dados analisados dos questionários aplicados aos clientes, 40,5% dos clientes inquiridos afirmam ter recebido comunicações por parte da CECV em matéria de cibersegurança, sendo que os restantes ou não receberam ou não lembram se receberam, como se segue na Tabela 9:

Tabela 9: Recebimento de Comunicações de cibersegurança da CECV

	Frequency	Percent	Valid Percent	Cumulative Percent
Sim	32	40,5	40,5	40,5
Não	22	27,8	27,8	68,4
Não me lembro	25	31,6	31,6	100,0
Total	79	100,0	100,0	

De acordo com as respostas dos inquiridos, 51,9% dos clientes inquiridos acham que não possuem informações suficientes para protegerem as operações realizadas *online*. Para suprir essa necessidade, 33,6% dos inquiridos obtém informações sobre cibersegurança através de notícias (*sites*, jornais, televisão, etc.), 32,2% utiliza as redes sociais para se informar e somente 18,5% recorre às comunicações da CECV (Tabela 10).

Tabela 10: Fontes de informação de cibersegurança para clientes

Fontes de Informação	Responses	
	N	Percent
Comunicação CECV	27	18,5%
Redes Sociais	47	32,2%
Noticias (sites, jornais,…)	49	33,6%
Amigos e Familiares	20	13,7%
Internet	1	0,7%
Formação na área	1	0,7%
Nenhuma	1	0,7%
	146	100,0%

A pouca informação sobre a cibersegurança por parte de clientes espelha-se no conhecimento dos inquiridos em relação a ataques cibernéticos. Cerca de 23,2% afirmam que não conhecem nenhum ataque cibernético, sendo que *malware* (29,6%) é o ataque mais conhecido pelos clientes inquiridos (Tabela 11).

Tabela 11: Conhecimento dos clientes sobre ataques cibernéticos

Ataques cibernéticos	Responses	
	N	Percent
Engenharia Social	29	23,2%
Malware	37	29,6%
Ransomware	21	16,8%
Ataques DDoS	9	7,2%
Nenhuma	29	23,2%
	125	100,0%

Outro ponto importante nesta categoria tem haver com o trabalho remoto. Esta modalidade foi adotada pela CECV durante o período da pandemia onde surgiram um conjunto de condicionalidades e desafios. Por sorte, a pandemia coincidiu com um momento em que a CECV passava por "processos de transformação digital (…) com forte aposta na disrupção de dependência de fornecedores externos através da criação de uma equipa de desenvolvimento interno" (I1). Durante os períodos de confinamento, por forma a continuar a fornecer os serviços bancários, considerados essenciais para a sociedade, a CECV criou condições para o trabalho remoto, principalmente dos serviços centrais. A instituição "disponibilizou computadores portáteis para alguns colaboradores (…) e instalou VPN's" (I1), reunindo condições para que a "CECV fosse o único banco em que todos dos serviços centrais trabalhassem remotamente" (I1). Para garantir a operacionalidade do trabalho remoto estabeleceu-se "reuniões de avaliações diárias e semanais" e criou-se uma "comissão de segurança para suporte e avaliar o estado dos trabalhos" (I1).

4.3.3. Físicas

Esta categoria destina-se à análise das principais infraestruturas físicas da CECV e as medidas adotadas para garantir a segurança do ambiente físico da instituição.

Em relação às principais infraestruturas da instituição, a CECV possui um "*data center* principal *inhouse* (…) acompanhado de um *data center* de *disaster recovery"* (I3) que "recebe *backups* diários e replicação em tempo real do nosso core bancário e todos os nossos sistemas" (I1) por forma a garantir a continuidade. Quanto aos equipamentos, a instituição possui um "parque informático, em termos de tecnologias e arquitetura rede, modernizado recentemente" (I1), dispõe de "equipamentos do sistema do *core*

bancário, equipamentos de virtualização, entre outros" (I3), além dos equipamentos de rede com "ligação fibra para todas as agências e com o parceiro interbancário SISP" (I3), recentemente melhoradas com "largura de bandas mais fiáveis" (I1). No que toca aos servidores físicos, recentemente substituídas como refere o Relatório e Contas 2023, além dos servidores de gestão de acessos e identidades, a instituição possui "servidores de suporte ao pessoal de segurança física, de vigilância, etc." (I3). Os principais servidores são "replicados no *data center disaster recovery* para garantir a continuidade do negócio" (I3). Todas essas infraestruturas são assistidas pelos "serviços de suporte à rede, nomeadamente antivírus, manutenção de infraestruturas, gestão de *logs*, algumas aplicações a volta do negócio (gestão de créditos, gestão de operações, aplicações de comunicação com os clientes, avaliação de desempenho, gestão de projetos, etc.)" (I3). Uma das políticas defendidas pela CECV em relação aos equipamentos passa pela manutenção preventiva e corretiva dos equipamentos, como referem no mais recente Relatório e Contas 2023, procurando sempre estar o mais atualizado possível, com "equipamentos da linha da frente em relação à realidade" (I1). A instituição ainda assume o compromisso de continuar a melhorar as infraestruturas, sendo que no mesmo relatório referem a existência de um projeto para uma nova Central de Riscos.

Todas essas infraestruturas físicas, são monitorizadas através de sistemas de vídeo como mencionado anteriormente na categoria Organizacional, além dos "sistemas automáticos de estimação de incêndio" (I3). Os equipamentos, tanto dos postos de trabalho como dos servidores, estão equipados com "antivírus que recebem atualizações de forma automática" (I3). Importante referir que a CECV segue a regra da mesa/secretária limpa nas suas instalações, isto é, "não deixar documentos que podem conter dados confidenciais em cima da mesa de trabalho" (I3).

4.3.4. Tecnologias

Esta categoria trata da análise das principais tecnologias, incluindo aplicações, da CECV e bem como das estratégias para assegurar a proteção dessas tecnologias, tendo em conta a grande importância que desempenham na atividade da instituição e no fluxo de informação e dados.

Como já mencionado na categoria das medidas Físicas, a CECV possui uma vasta gama de tecnologias para garantir as suas atividades, desde servidores de rede, sistemas operativos e aplicações à volta do *core business* bancário, a instituição possui igualmente várias medidas para garantir a proteção dessas tecnologias. Desde já a instituição encontra-se num processo de "migração das aplicações web do core bancário para *https*" (I3) garantindo um ambiente seguro e de confiança aos colaboradores enquanto utilizadores. Para prevenção de intrusões, a instituição utiliza "*firewalls* de nova geração" (I3) que também desempenham funções de "antivírus, controlo de aplicações e filtragem de endereços" (I3). De referir que todos os sistemas operativos dos utilizadores "recebem *updates* regulares e de segurança" (I3), seguindo a política de estar sempre atualizado. Nesse sentido, o Relatório e Contas 2023 destaca a atualização dos sistemas de segurança eletrónica e a renovação de licenciamentos como Microsoft, Office, HP, McAfee, RPA, Apple/Google entre outros.

Sendo uma instituição que aposta fortemente no digital, a CECV oferece aos seus clientes vários serviços digitais: *Homebanking* CaixaNet, *App* Caixa Mobile, Plataforma Crédito Digital e *App* Caixa Microcrédito. Todas essas aplicações são "disponibilizados aos clientes na internet em *http* e com certificado digital de garantia de segurança" (I3). O foco da análise será a aplicação CaixaNet que se trata de uma aplicação "montada e desenhada por pessoas externas" (I1). De acordo com dados recolhidos do questionário, a aplicação tem mostrado ser bastante útil para os clientes. A maioria dos inquiridos (36,7%) utiliza a aplicação diariamente, 34,2% utiliza-a semanalmente e 15,2% dos clientes utiliza-a pelo menos mensalmente, como demostra a Tabela 12:

Tabela 12: Frequência de utilização da CaixaNet

	Frequency	Percent	Valid Percent	Cumulative Percent
Diariamente	29	36,7%	36,7	36,7
Semanalmente	27	34,2%	34,2	70,9
Mensalmente	12	15,2%	15,2	86,1
Raramente	7	8,9%	8,9	94,9
Nunca	4	5,1%	5,1	100,0
Total	79	100,0%	100,0	

A CaixaNet oferece um conjunto de utilidades, sendo que de acordo com o último Relatório e Contas 2023, as transações mais realizadas foram consultas de saldo,

transferência intrabancárias, pagamento de serviços e carregamentos de telemóvel. Os dados recolhidos dos questionários confirmam essas informações, sendo a consulta de saldo e movimentos a funcionalidade mais utilizada pelos clientes (38,7%), seguido das transferências bancárias (37,6%) e pagamento de contas (19,1%). Aplicações financeiras e carregamento de telemóvel foram as menos utilizadas, como representada na Tabela 13:

Tabela 13: Serviços CaixaNet mais utilizadas

	Responses	
	N	**Percent**
Consulta Saldo e Movimentos	67	38,7%
Transferências bancárias	65	37,6%
Pagamentos de contas	33	19,1%
Aplicações Financeiras	5	2,9%
Carregamento Telemóvel	2	1,2%
Nenhum	1	,6%
Total	173	100,0%

Com vista a reforçar a segurança dos clientes no acesso às funcionalidades de *internet banking*, a CECV implementou a ferramenta "*one-time password*" (I1), reduzindo as tentativas de ataques cibernéticos, nomeadamente *phishing.* De destacar que quase todos os clientes inquiridos (84,8%) sentem-se seguros ou muito seguros na utilização desses serviços de *internet banking* fornecidos pela CECV através da CaixaNet. Somente 13,9% dos inquiridos posiciona-se neutro quanto à segurança e apenas 1,3% sente-se de facto muito inseguro, como se segue apresentado na Tabela 14:

Tabela 14: Nível de segurança dos utilizadores de CaixaNet

	Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Muito Seguro	14	17,7%	17,7	17,7
Seguro	53	67,1%	67,1	84,8
Neutro	11	13,9%	13,9	98,7
Muito Inseguro	1	1,3%	1,3	100,0
Total	79	100,0%	100,0	

Outro aspeto de extrema importância considerado na avaliação tecnológica da CECV tem haver com os processos de backup. A CECV possui "ferramentas de *backups* diários e de replicação em tempo real do core bancário e de todos os sistemas bancários"

(I1). Essas operações de *backups* e replicação de dados é garantido por "uma aplicação que interage com o sistema de virtualização da instituição" (I3) e envia a cópia para o *disaster recovery*. Para salvaguarda de dados, a instituição guarda dados seguindo a "regra 3-2-1: 3 cópias de dados em 2 meios diferentes e pelo menos 1 guardado em outro espaço físico" (I3). Assim, faz-se "cópias para tapes e cópias para discos, e uma dessas cópias fica no *disaster recovery*" (I3).

Em relação ao sistema de email da CECV é "delegado ao provedor de serviço na *cloud* (…) com mecanismos de segurança de *antisspam*, *antimalware*, *antiphishing"* (I3). Recentemente, a instituição reforçou a segurança do sistema emails completando "trio de controlo SPF, DKIM e DMARC" (I3), uma vez que os emails têm sido dos canais mais frequentes utilizados por invasores.

4.3.5. Certificação ISO 27001

Sendo um dos objetivos do estudo avaliar o processo e os impactos da obtenção da certificação ISO 27001, ao longo desta categoria serão analisados os dados por forma a retirar conclusões que permitam atingir esses objetivos.

Iniciado em 2008, a "CECV iniciou um processo de auditoria complexo de segurança de informação, culminando em 2012 com a certificação ISO 27001 (…) pela empresa Bureau Veritas" (I1) portanto, o processo de certificação "demorou 4 anos" (I1). Desde 2008 foram feitos vários esforços, investimentos e mudanças no seio da instituição para que se cumprisse com os requisitos do normativo, caraterizada como sendo essencialmente uma "mudança de paradigma drástica" (I1). "Além de investimentos em tecnologias e equipamentos, eram necessários investimentos em termos de procedimentos, normativos, reengenharia de processos, boas práticas" (I1).

No ano que antecede à certificação, apesar de existir na CECV "um departamento de auditoria interna, esta não tinha o trabalho de auditoria de informática" (I1), por isso os investimentos eram alvos de auditorias informáticas com apoio de consultor externo, como refere o Relatório e Contas 2011. Segundo este mesmo documento, em 2011 consolidou-se a implementação das recomendações no âmbito da ISO 27001 com a criação do Gabinete de Segurança, conclusão da criação da documentação para ISO 27001 e inventariação da segurança física, além de investimentos na tecnologia e

informática (reforço da equipa com mais 2 técnicos, materialização da área de Redes e Sistemas, entre outros).

Em 2012, a CECV foi certificada com a ISO 27001, mas também a ISO 9001 (Gestão de Qualidade). Segundo os dados do Relatório e Contas 2012, nesta altura a CECV foi o primeiro banco em Cabo Verde com as duas certificações, segundo a nível da CPLP e quarto em toda a África, o que demonstra a grandiosidade desse feito. Neste período consolidou-se vários projetos, desde já com destaque para a auditoria de segurança dos sistemas de informação e implementação das recomendações, mas também a formação de colaboradores em segurança de infraestrutura tecnológica. Outras ações foram realizadas: migração do *data center*, upgrade, substituição e reconfiguração de equipamentos de comunicação.

Um ano após a certificação, de acordo com os dados do Relatório e Contas 2013, continuou-se a consolidação das recomendações, sendo que a CECV foi alvo da primeira auditoria de acompanhamento da ISO 27001 que evidenciou ainda necessidades de implementação de alguns controlos, maioria associados a procedimentos. Fruto dos requisitos da ISO, foram substituídos todos os computadores de *front office* da instituição.

Desde então até os dias de hoje, a CECV tem feito um conjunto de investimentos e mudanças por forma a corresponder às boas práticas exigidas pelo normativo e renovar a certificação. Um dos grandes investimentos realizados foi a "modernização recente do parque tecnológico, incluindo os sistemas e a arquitetura de rede, com o objetivo de estar em *compliance* com as boas práticas internacionais" (I1).

Muitos foram os desafios para conquistar e manter a certificação, nomeadamente os "hábitos das pessoas" (I1) uma vez que lhes "obriga a ter certas posturas de segurança" (I3). A ISO 27001 "não se cinge à parte tecnológica, abrange também os recursos humanos" (I3). Normalmente, alguns colaboradores mostraram alguma resistência visto que "houve mudanças no modo de fazer coisas, por exemplo: pedidos de acesso, revisão de acessos, ferramentas de *ticketing*, montagem de KPI's (indicadores de performance), etc." (I1). Outro exemplo de resistência dos colaboradores prende-se com a "política de não impressão, onde tem gerado alguns conflitos pela não disponibilização de impressoras em algumas salas de colaboradores" (I1). A certificação implicou maior controlo na "entrada e saída de pessoas, na forma como é

feita o descarte de dados, seja digital ou em suporte papel, na forma como os utilizadores se comportam com os dados pessoais dos clientes (a regra de mesa/secretária limpa)" (I3). De acordo com os dados recolhidos da amostra de colaboradores, todos (100%) mostraram-se cientes da certificação da CECV pela norma ISO 27001, sendo que 60% admitem utilizarem sempre os procedimentos implementados pelo normativo no desempenho das funções diárias e os restantes 40% utilizam frequentemente esses procedimentos, como demostra a Tabela 15. Esses números mostram a boa penetração das medidas da ISO 27001 na CECV e a aceitação das mesmas por parte dos colaboradores.

Tabela 15: Frequência de utilização de procedimentos ISO 27001

Frequência de utilização de procedimentos ISO 27001	Ciente de que a CECV é certificada		Total
	N	Percent	
Sempre	9	60%	9
Frequentemente	6	40%	6
Total	15	100%	15

Contudo, em relação aos clientes o cenário é contraditório. Uma maioria esmagadora (cerca de 77,2%) não sabe que a CECV é um banco certificado pela ISO 27001 Segurança de Informação (Tabela 16).

Tabela 16: Conhecimento dos clientes em relação à certificação

	Frequency	Percent	Cumulative Percent
Sim	18	22,8	22,8
Não	61	77,2	100,0
Total	79	100,0	

Infelizmente não foi possível obter informação quantitativa em relação aos custos do processo de certificação. Mas pode-se considerar que todos esses investimentos e esforços tiveram "custos enormes, desde contratação de consultores externos, auditorias, viagens, investimentos tecnológicos, documentação, formação no estrangeiro *Lead Implementer* da ISO27001 para técnico específico do banco, etc." (I1).

Relatado no Relatório e Contas 2023, a CECV continua sendo "o único banco em Cabo Verde certificado com a ISO 27001 (…) o que tem permitido estar um pouco na linha da frente no que diz respeito à segurança física e eletrónica, avaliação do plano de continuidade negócios, investimentos tecnológicos e formação das pessoas" (I1). A certificação ISO 27001 é um claro sinal de que "a CECV está preocupada com a questão da cibersegurança e proteção de dados pessoais" (I3) o que traduz em benefícios tanto para a CECV, mas também para os clientes. O normativo tem "um *scope*/âmbito que é essencialmente garantir que os nossos dados e os dados dos nossos clientes nunca sejam comprometidos" (I1). Um dos principais benefícios para a CECV é que a certificação é vista como uma "prova de diferenciação em relação aos concorrentes" (I1), o que traz impactos na "confiança dos clientes e dos investidores" (I1). Dados recolhidos da amostra de clientes confirma essa afirmação. Cerca de 29,1% dos inquiridos admitem que pelo facto da CECV ser um banco certificado pela ISO 27001 aumenta significativamente a sua confiança no banco e 46,8% admite aumentar moderadamente a sua confiança, como se apresenta na Tabela 17:

Tabela 17: Impacto da certificação ISO 27001 na confiança dos clientes

	Frequency	Percent	Cumulative Percent
Sim, significativamente	23	29,1%	29,1
Sim, moderadamente	37	46,8%	75,9
Neutro	18	22,8%	98,7
Não, pouco	1	1,3%	100,0
Total	79	100,0%	

Outro grande benefício resultante dos procedimentos implementados pela ISO 27001 tem haver com a "melhoria nos processos" (I1) e nos "desempenhos de cibersegurança" (I3), causado pela exigência de iniciativas de melhoria continua. Os próprios colaboradores confirmam através dos dados quantitativos. 73,3% dos colaboradores inquiridos afirmam que a implementação da certificação trouxe melhorias significativas na segurança das informações do banco e dos clientes, os restantes 26,7% inquiridos concordam que houve melhorias moderadamente (Tabela 18).

Tabela 18: Perceção dos funcionários sobre melhorias trazidas pela ISO 27001 na segurança da informação

	Frequency	Percent	Cumulative Percent
Sim, significativamente	11	73,3	73,3
Sim, moderadamente	4	26,7	100,0
Total	15	100,0	

Resumidamente, as melhorias trazidas pela certificação ISO 27001 enquadram-se em 3 grandes grupos: "Melhoria da reputação da instituição, melhoria nas operações do dia a dia da CECV e melhoria do aspeto tecnológico" (I3).

4.3.6. Preocupações, Ameaças e Sugestões

Esta categoria destina-se à análise das preocupações e das principais ameaças cibernéticas à CECV, sabendo que os riscos cibernéticos são uma realidade bem presente. Também se aborda as sugestões de possíveis melhorias nas estratégias de mitigação desses riscos.

Tendo em conta que a CECV é uma instituição crítica no sistema financeiro de Cabo Verde e considerando a própria natureza sistémica do sistema económico-financeiro, a cibersegurança de todo o sistema e dos seus participantes é de extrema importância. Alinhado com a revisão de literatura feita anteriormente, destaca-se o facto de que "em Cabo Verde não existe um CSIRT (…), não existe colaboração entre instituições, não há partilha de e troca de informações (…)" (I1), impossibilitando a aprendizagem com "acontecimentos passados e erros cometidos por outras instituições" (I1).

Como visto nas categorias anteriores, várias são as estratégias adotadas para mitigar as vulnerabilidades existentes na instituição. Os "30 centímetros: distância entre o computador e o utilizador" (I1) continuam sendo dos maiores desafios enfrentados por todas as instituições, precisamente por ser um dos maiores vetores de ciberataques. De acordo com dados da amostra de colaboradores, cerca de 50% dos inquiridos consideram a Engenharia Social (*phishing/smishing/vishing)* como a maior ameaça cibernética, seguido do *Malware* (20,8%) e *Ransomware* (20,8%) (Tabela 19).

Tabela 19: Maiores ameaças cibernéticas, segundo os colaboradores

	Responses	
	N	Percent
Engenharia Social	12	50,0%
Malware	5	20,8%
Ransomware	5	20,8%
Ataques DDoS	2	8,3%
Total	24	100,0%

Já os entrevistados indicam o *Ransomware* como "um dos maiores desafios" (I3) enfrentados pela CECV devido proliferação pelo canal de email. Por isso consideram importante a "sensibilização dos trabalhadores e a proteção do sistema de emails" (I3). Também a "migração sequencial de dados e aplicações para *cloud*" (I3) é uma preocupação uma vez que "as políticas de segurança utilizadas atualmente não contemplam essa nova realidade" (I3). Por último a "complexidade no geral de toda a tecnologia de suporte ao digital" (I3) representa um grande desafio visto que "obriga o pessoal técnico a estar constantemente atualizado" (I3).

Perante essas ameaças, os colaboradores inquiridos mostram-se preocupados com os riscos cibernéticos à volta da CECV. A maioria dos inquiridos, cerca 46,7% afirmam estar muito preocupados em relação aos riscos cibernéticos, sendo que apenas 6,7% mostraram-se pouco preocupados, como se apresenta na Tabela 20. O *core business* da CECV e o *home banking* foram identificados como "áreas que se tem maior preocupação (…) por serem o motor da sustentabilidade de todo o negócio da CECV" (I2).

Tabela 20: Nível de preocupação dos colaboradores em relação a riscos cibernéticos na CECV

	Frequency	Percent	Cumulative Percent
Muito preocupado(a)	7	46,7%	46,7
Preocupado(a)	6	40,0%	86,7
Neutro(a)	1	6,7%	93,3
Pouco preocupado(a)	1	6,7%	100,0
Total	15	100,0%	

Levando em consideração as preocupações, é sempre necessário identificar áreas de melhorias. Claramente que "uma boa capacidade de resiliência é o ponto de chegada" (I3) para os esforços da CECV, reconhecendo que "nunca se consegue chegar a um ponto de perfeição" (I3) havendo sempre "novas oportunidades de melhoria" (I3).

"Mais ações de formação, mais sessões de sensibilização, realização de simulacros anónimos, etc." (I1) são alguns dos pontos identificados como suscetíveis de melhorias. Os dados dos funcionários confirmam que a formação e a sensibilização são as áreas das estratégias de mitigação de riscos cibernéticos da CECV que necessitam de melhorias, seguidas pelas tecnologias de segurança (Tabela 21). É importante mencionar que já existe uma proposta para a realização de ações de "*ethical hacking*" (I1), que consiste na deteção de vulnerabilidades cibernéticas na instituição.

Tabela 21: Áreas de melhorias nas estratégias da CECV, segundo os funcionários

	Responses	
	N	**Percent**
Políticas e procedimentos	5	10,4%
Plano de resposta a incidentes	6	12,5%
Formação e consciencialização	12	25,0%
Tecnologias de segurança	10	20,8%
Monitorização a incidentes	7	14,6%
Auditorias e Avaliações	7	14,6%
Outro (Atitude)	1	2,1%
Total	48	100,0%

Tendo em conta o papel importante do *home banking* na sustentabilidade da instituição, a sua segurança é imprescindível. De acordo com dados da amostra dos clientes em relação às medidas de segurança no serviço *internet banking*, 38,4% dos inquiridos pediram mais alertas em tempo real no *home banking* e na aplicação, 25,8% dizem precisar de mais informações sobre cibersegurança nesses produtos e 21,2% identificaram a autenticação multifator como uma possível medida a ser implementada (Tabela 22). Da análise de dados das sugestões e comentários, os clientes apontaram outras medidas de melhorias necessárias: aumento do número de dígitos para escolha da chave de confirmação; envio do código de confirmação para email ao invés de o enviar para o número de telemóvel; melhorar a plataforma e o aplicativo da CaixaNet. Também algumas críticas foram feitas em relação a funcionalidade da CaixaNet.

Alguns clientes afirmam ser um aplicativo muito instável, uma vez que nem sempre consegue-se ter acesso, e que algumas funcionalidades deixam de dar resposta após o horário normal de funcionamento.

Tabela 22: Medidas de segurança na internet banking sugeridas por clientes

	Responses	
	N	**Percent**
Autenticação Multifator	32	21,2%
Alertas em tempo real	58	38,4%
Melhorias na interface	21	13,9%
Mais informações	39	25,8%
Nenhuma	1	0,7%
Total	151	100,0%

Outros comentários foram feitos em relação às boas práticas na CECV, por exemplo evidenciou-se a necessidade de a instituição reforçar as medidas preventivas no combate às ameaças cibernéticas. Uma nota para um comentário interessante que destaca o facto de, contrariamente às boas práticas internacionais, a Direção de Informática, Comunicação e Segurança ser responsável simultaneamente pela Informática e pela Segurança Informática.

Importa referir melhorias sugeridas para o setor financeiro nacional, que "merece uma atenção especial" (I1). Pelo facto de não existir "um CSIRT nacional (…) devia-se avançar para um CSIRT financeiro. Isto é, todos os bancos terem um centro de monitorização que reporta situações que acontecem na área financeira" (I1) uma vez que se nota a falta de cooperação entre as instituições financeiras em matéria de cibersegurança.

5. CONCLUSÃO

Ao longo deste capítulo serão enunciadas as principais conclusões do estudo realizado, as suas limitações e sugestões para futuras investigações. Também será feita uma breve consideração final quanto à elaboração da dissertação.

5.1. PRINCIPAIS CONCLUSÕES SOBRE O ESTUDO

Para apresentar as conclusões relativo ao estudo apresentado, será seguido o mesmo raciocínio do capítulo anterior. As conclusões serão apresentadas de acordo com as categorias de análise de resultados definidas: Organizacional; Pessoas; Físicas; Tecnologia; Certificação ISO 27001.

Com recurso a análise dos dados recolhidos das duas entrevistas, dos dois questionários e dos Relatório e Contas (2011, 2012, 2013 e 2023) e considerando os objetivos do estudo definidos inicialmente na metodologia de investigação, foi possível extrair importantes conclusões.

A nível de medidas organizacionais, tendo em conta o exposto na análise dos resultados do estudo, nota-se que a instituição dispõe de boas ferramentas de controlo de acesso e identidade em todas as infraestruturas. Destaca-se o sistema de controlo biométrico de entradas e acessos e a utilização da autenticação multifator no acesso dos colaboradores, seguindo recomendações internacionais. Em termos de monitorização, destaca-se os sistemas de monitorização de vídeo para controlo do acesso físico e o sistema de *logs*, responsável pela monitorização e armazenamento de todos os *logs* dos sistemas, o que garante uma boa avaliação em termos de monitorização de toda a instituição. Quanto aos procedimentos e políticas adotadas, a CECV tem implementado um conjunto de medidas que proporcionam um ambiente cibernético seguro, com destaque para múltiplos processos anuais de auditorias (internas e externas). No que toca à documentação e normativos, pode-se dizer que a instituição esteja bem avaliada uma vez que possui um conjunto de documentos (normas, manuais, procedimentos e registos), revistos anualmente, que garantem a disponibilização das informações necessárias aos colaboradores. De referir a existência do Plano de continuidade de negócio e Plano de recuperação, segundo recomendações internacionais. Contudo, a nível de parcerias e partilha de informação em matéria de cibersegurança, identifica-se

uma vulnerabilidade na instituição. Fraca cooperação entre as instituições financeiras é o ponto fraco das medidas organizacionais, muito influenciado pelo fraco contexto nacional de cibersegurança. Com isso, apesar da vulnerabilidade organizacional identificada, pode-se afirmar que a CECV esteja bem avaliada a nível de estratégias organizacionais.

Quanto às estratégias relacionadas com as pessoas, verificou-se que a CECV é uma instituição que investe fortemente na formação interna e externa dos seus colaboradores com várias iniciativas nesse sentido, como verificadas na análise dos resultados do estudo. Contudo, os dados recolhidos mostram que uma grande parte dos colaboradores afirmaram que não recebem formações em cibersegurança por parte da CECV, sendo que as formações ministradas não acontecem regularmente, como mandam as boas práticas internacionais. Com esses dados, permite-nos estabelecer uma relação quanto à neutralidade da maior parte dos colaboradores quando questionados sobre a sua satisfação em relação às formações da CECV em cibersegurança. Não obstante, a falta de ações de formação em cibersegurança, os colaboradores mostraram bons níveis de conhecimentos sobre ataques cibernéticos o que poderá estar relacionado com as ações de sensibilização feitas pela instituição, nomeadamente na entrada de novos colaboradores, no programa "Comunica Comigo" e nas ações *online* bianuais do responsável pela segurança em matéria de segurança de informação. Posto isto, pode-se concluir que apesar dos muitos investimentos feitos em formação, a cibersegurança não tem sido um dos temas mais frequentes ou, uma outra possibilidade, não tem abrangido todas as áreas da instituição. Quanto aos clientes da instituição, nota-se que maior parte dos clientes afirma nunca ter recebido ou não se recorda de ter recebido informações e ações de sensibilização sobre boas práticas de segurança cibernética. Com isso, pode-se concluir que as iniciativas de cibersegurança da CECV para os clientes têm mostrado ser insuficientes, com a maior parte dos clientes a afirmarem não ter informações suficientes para proteção nas atividades bancárias *online*. Em termos de trabalho remoto, durante a pandemia, a instituição criou as condições necessárias para continuar a sua atividade, sendo de destacar que 100% dos serviços centrais estiveram em trabalho remoto. Não se conseguiu obter informações quanto à atualidade.

Resumindo, em termos de estratégias em relação aos colaboradores e clientes, a instituição encontra-se com uma avaliação pouco favorável, representando uma

vulnerabilidade nas estratégias globais, sendo a formação e consciencialização a área da CECV que mais precisa de melhorias, segundo os colaboradores inquiridos.

A nível das medidas físicas, constata-se que a CECV possui infraestruturas modernas devido aos investimentos que tem vindo a realizar em prol da transformação digital. Das infraestruturas analisadas, uma nota para a existência de um *data center* principal acompanhado de um *data center* de *disaster recovery*, muito importante para garantir a continuidade da atividade, seguindo as boas práticas internacionais. A instituição defende uma política de estar sempre atualizada e, neste sentido, possui um parque informático (rede e sistemas) moderno e de acordo com as recomendações, servidores físicos recentemente substituídos, entre outros equipamentos. Os equipamentos e as infraestruturas são alvos de manutenção preventiva, mais uma vez, seguindo as boas práticas. Importante referir a adoção da regra "mesa/secretária limpa" no combate ao vazamento de dados confidenciais. Todas essas infraestruturas permitem concluir que a CECV está avaliada positivamente em termos de medidas de estratégias físicas, aumentando a sua resiliência cibernética.

Quanto ao tópico das estratégias com foco nas tecnologias, nota-se que a CECV utiliza *firewalls* e antivírus atualizados periodicamente e com licenças renovadas, que garantem a segurança das tecnologias e do fluxo de informação que circula nelas. Seguindo sempre as boas práticas de estar sempre atualizada, a instituição procura também manter os sistemas operativos atualizados e com licenças válidas. O aplicativo de *internet banking* CaixaNet mereceu atenção por ser considerado um dos motores da sustentabilidade do negócio da CECV. Uma aplicação com certificado digital de garantia de segurança, utilizada diariamente pela maioria dos clientes e considerada segura pelos seus utilizadores, principalmente após implementação da ferramenta *one-time password*. Contudo, os utilizadores relatam ser um aplicativo instável devido à impossibilidade de realizar determinadas operações fora do horário de funcionamento da instituição. Um aspeto a merecer atenção por parte da instituição, juntamente com implementação de alertas de cibersegurança a tempo real. Dos aspetos mais relevantes no que toca a resiliência cibernética de uma instituição, tem haver com o sistema de *backup*. A CECV, neste sentido, mostra-se relativamente bem preparada com o sistema de *backup* diários do *core* bancário e de replicação dos servidores, seguindo a regra de boas práticas 3-2-1. Isto é, a instituição realiza 3 cópias de dados, em 2 meios diferentes (*tapes* e disco) e 1 delas guardado em um lugar físico distinto, no *disaster recovery*

mais precisamente. Considerado o canal mais utilizado pelos cibercriminoso, o sistema de email da CECV é considerado robusto, encontrando-se delegado na *cloud* com mecanismos de *antispam*, *antimalware* e *antiphishing*. Além disso a instituição completou recente a trio de controlo SPF, DKIM e DMARC, considerado internacionalmente como um importante instrumento de segurança do serviço de correio eletrónico com foco nos domínios. Posto isto, pode-se concluir que a nível de tecnologias a CECV possui boas estratégias de mitigação de riscos cibernéticos.

Analisadas todas as categorias definidas para a avaliação da eficácia das estratégias de mitigação de riscos cibernéticos da CECV permite-nos concluir que: apesar da vulnerabilidade identificada na formação e consciencialização dos colaboradores em matéria de cibersegurança, **as estratégias de mitigação de riscos cibernéticos da CECV são eficazes.** Esta conclusão é suportada por todas as medidas mencionadas na análise, resultando no facto da CECV nunca ter sofrido um ataque cibernético com impactos significativos, prova da eficácia dessas estratégias. É ainda suportada pelo facto de em todas as auditorias de sistemas de informações realizadas na instituição, nunca se ter identificado uma "não conformidade maior".

No que diz respeito à análise da certificação ISO 27001, conclui-se que o processo, que demorou 4 anos, representou essencialmente uma mudança drástica de paradigma, implicando a adoção de novos procedimentos, reengenharia de processos e implementação de boas práticas. Este processo trouxe, e continua a trazer, desafios, sendo o maior deles a resistência das pessoas, uma vez que houve mudanças nos hábitos e no modo de trabalhar. A certificação da ISO 27001 resultou de um conjunto de investimentos em documentação, procedimentos, boas práticas e, principalmente, em tecnologias e equipamentos, com destaque para a modernização de todo o parque tecnológico (rede e sistemas). Além desses investimentos, foram necessárias consultorias, auditorias, formações, viagens, entre outros, resultando em "custos enormes" que não puderam ser quantificados por falta de informações quantitativas.

A certificação visa essencialmente garantir a segurança das informações e dados do banco e dos seus clientes. Esta trouxe melhorias nos processos do dia a dia da instituição e no desempenho em termos de cibersegurança, como demonstrado pelos dados recolhidos, nos quais todos os colaboradores afirmam utilizar as medidas implementadas pela ISO 27001 nas suas funções e reconhecem que estas resultam em

melhorias. A certificação também melhorou a reputação da CECV, destacando-a como uma instituição que se preocupa com a segurança dos dados dos seus clientes, o que proporcionou um aumento da confiança por parte dos mesmos, como evidenciado pelos dados quantitativos. Além disso, houve melhorias no aspeto tecnológico devido aos investimentos já mencionados.

Contudo, um ponto menos positivo prende-se com a pouca divulgação do facto de a instituição ser certificada pela ISO 27001, ainda mais sendo o único caso no mercado. O pouco aproveitamento deste facto é comprovado pelos dados quantitativos, nos quais a grande maioria dos clientes desconhecia que a instituição era certificada pela ISO 27001.

Tendo em conta algumas vulnerabilidades e pontos menos fortes identificados na CECV ao longo das análises, propõe-se as seguintes melhorias:

- Mais sessões de formação e consciencialização para colaboradores de todas as áreas da CECV;
- Aumento de ações cibersegurança junto dos clientes, nomeadamente campanhas de sensibilização e divulgação frequente de informações;
- Maior divulgação da certificação ISO 27001 e aproveitamento como ponto de atração e diferenciação no mercado;
- Inclusão do tratamento das ferramentas *cloud* nas políticas da CECV;
- Estabelecimento de parcerias com instituições locais e reguladores, nomeadamente ARME e NOSi, visando formações e promoção de partilha de informações e boas práticas de cibersegurança.

5.2. LIMITAÇÕES DO ESTUDO

O estudo realizado, apesar de fornecer conclusões valiosas sobre os objetivos propostos, apresentou algumas limitações. A identificação dessas limitações é importante para compreensão do alcance dos resultados, bem como orientar futuras investigações na área.

As principais limitações do estudo encontram-se relacionadas com as amostras, dos clientes e dos colaboradores. Tendo em conta que a fraca adesão dos colaboradores da instituição aos questionários e a não possibilidade de distribuição dos questionários aos

clientes pelos seus canais da instituição, as amostragens foram selecionadas por conveniência. O que traz incertezas quanto à extrapolação, com uma certa confiança, dos resultados das amostras para as populações. Com isso, as dimensões das amostras poderão não ser consideradas significativas.

Outra limitação relacionada com a amostra dos clientes, relaciona-se com o alcance de empresas clientes da CECV. A amostra dos clientes foi constituída praticamente na totalidade por clientes particulares. Esta limitação justifica-se pela dificuldade de contacto com empresas para disponibilização do questionário.

Em relação aos documentos pretendidos para o estudo, foi limitado pelo facto de grande parte dos documentos serem de caráter interno e confidenciais. Tendo em conta a natureza do estudo, compreende-se perfeitamente a decisão da instituição, relembrando que durante todo o estudo procurou-se respeitar sempre a confidencialidade dos dados.

5.3. SUGESTÕES PARA FUTURAS INVESTIGAÇÕES

Com base nos resultados obtidos e nas limitações identificadas, surgem oportunidades de melhorias para pesquisas futuras sobre os riscos cibernéticos não só na instituição do estudo (CECV), mas também outras instituições do ramo.

Desde já a escolha de amostras mais significativas, levando em conta métodos de amostragem mais sofisticados e complexos. Amostragens mais significativas permitem a extrapolação de resultados para a população com maior nível de certeza, permitindo retirar valiosas conclusões por forma a melhorar o objeto de estudo.

Seria interessante, a realização de um estudo sobre o contexto cibernético do mercado bancário Cabo-verdiano, tendo em conta ser um tema ainda por explorar na realidade desse país e o facto dos bancos desempenharem um papel crucial no sistema financeiro nacional.

5.4. CONSIDERAÇÕES FINAIS

O presente estudo teve como objetivos avaliar a eficácia das estratégias de mitigação dos riscos cibernéticos na CECV, identificar vulnerabilidades e sugerir melhorias nas mesmas, e ainda estudar o processo e os benefícios trazidos pela certificação ISO 27001.

Com recurso à revisão de literatura, foi possível compreender a realidade e adquirir conhecimentos importantes relacionados com o tema, de forma a orientar melhor a investigação. Através de entrevistas, questionários e documentos, foi possível chegar a conclusões em relação aos objetivos propostos.

Concluiu-se que, as estratégias de mitigação de riscos cibernéticos da CECV são eficazes, sendo que se identificou vulnerabilidades principalmente a nível de formação de colaboradores. Para o efeito propôs-se algumas melhorias que poderão ser implementadas por forma a reforçar a cibersegurança da instituição.

Foi possível verificar que o processo de certificação da instituição com ISO 27001 englobou desafios e foi custoso devido a vários investimentos efetuados pela CECV, sem poder quantificar valores. Resultou em benefícios de cibersegurança para a instituição e para os clientes, nomeadamente aumento da confiança de clientes, melhorias tecnológicas e melhorias nos processos.

A realização deste trabalho de dissertação representou, para mim, um grande desafio, tendo em conta ser um tema cujo meu conhecimento era limitado. Contudo, foi encarado como uma excelente oportunidade de aprendizagem sobre os riscos cibernéticos e a cibersegurança, temas cada vez mais presentes nas várias áreas do nosso dia-a-dia. Possibilitou o aprofundamento de conhecimentos existentes sobre a matéria, mas essencialmente a aquisição de novos conhecimentos e novas competências.

REFERÊNCIAS BIBLIOGRÁFICAS

Adelmann, F., Elliot, J., Ergen, I., Gaidosch, T., Jenkinson, N., Khiaonarong, T., … Wilson, C. (2020). Cyber Risk and Financial Stability: It's a Small World After All. *IMF Staff Discussion Note*, Washington, DC. Disponível em https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2020/12/04/Cyber-Risk-and-Financial-Stability-Its-a-Small-World-After-All-48622

Alegria, A. V., Montoya, A. N., Loayza, J. L. M. & Armas-Aguirre, J. (2022). Method of Quantitative Analysis of Cybersecurity Risks Focused on Data Security in Financial Institutions. *17th Iberian Conference on Information Systems and Technologies (CISTI)*, Madrid, Spain, ppp. 1-7, Disponível em https://ieeexplore.ieee.org/document/9820198

Balão, S. (2014). As NTIC, o Ciberespaço e a "Imagem do Poder" - Uma análise ostrogorskiana da Política Global contemporânea. *Agenda Política, 2* (1), 204-233. Disponível em https://www.agendapolitica.ufscar.br/index.php/agendapolitica/article/view/34

Bardin, L. (1977). *Análise de Conteúdo.* Lisboa, Portugal: Edições 70, Lda

Biswas, B., Mukhopadhyay, A., Kumar, A., & Delen, D. (2023). A hybrid framework using explainable AI (XAI) in cyber-risk management for defence and recovery against phishing attacks. *Decision Support Systems, 177*. Disponível em https://doi.org/10.1016/j.dss.2023.114102

Camilo, J.A. de O. (2021). Gestão de pessoas: práticas de recursos humanos na era digital. [e-book]. Disponível em: https://books.google.pt/books?id=8RoeEAAAQBAJ&pg=PT173&dq=Gest%C3%A3o+de+pessoas:+pr%C3%A1ticas+de+recursos+humanos+na+era+digital&hl=pt%20PT&sa=X&ved=2ahUKEwjMg4GUxer7AhU1TKQEHR8KD5UQ6AF6BAgEEAI#v=onepage&q=Gest%C3%A3o%20de%20pessoas%3A%20pr%C3%A1ticas%20de%20recursos%20humanos%20na%20era%20digital&f=false

CECV. (2023). *Relatório e Contas 2023.* Caixa Económica de Cabo Verde. Disponível em https://directus-cms-uploads.s3-eu-west-1.amazonaws.com/production-caixa-net-org/b947ad71-2351-47a3-80cd-73313df040ac.pdf

CECV. (n.d.). *Caixa Económica de Cabo Verde*. Disponível em https://www.caixa.cv/institution

Cervo, A. & Bervian, PP. (2002). *Metodologia Científica.* São Paulo, Brasil: Pearson Education.

CNCS (2021). *Cibersegurança em Portugal: Sociedade 2021*. Observatório de Cibersegurança. Centro Nacional de Cibersegurança. Disponível em https://www.cncs.gov.pt/docs/relatorio-sociedade2021-observ-cncs.pdf

CNCS (2023). *Cibersegurança em Portugal: Riscos & Conflitos*. Observatório de Cibersegurança. Centro Nacional de Cibersegurança. Disponível em https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf

Conselho Europeu. (2018). *Convenção para a proteção das pessoas relativamente ao tratamento de dados de caráter pessoal (Convenção 108).* Disponível em https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2

Data Protection Africa. (2023). *Africa: AU's Malabo Convention set to enter force after nine years.* Disponível em https://dataprotection.africa/malabo-convention-set-to-enter-force/

Decreto-Lei nº 27/2023. B.O. da República de Cabo Verde. I Série-nº109 (20-10-2023) 2212-2232. Disponível em https://kiosk.incv.cv/V/2023/10/20/1.1.109.5416/p2212

Decreto-Lei nº 33/2007. B.O. da República de Cabo Verde. I Série-nº36 (24-09-2007) 670-689. Disponível em https://kiosk.incv.cv/1.1.36.345/

Decreto-Lei nº 44/2009. B.O. da República de Cabo Verde. I Série-nº42 (09-11-2009) 975-979. Disponível em https://kiosk.incv.cv/1.1.42.215/

Decreto-Lei nº 9/2021. B.O. da República de Cabo Verde. I Série- nº9 (29-01-2021) 200-206. Disponível em https://kiosk.incv.cv/1.1.9.3589/

Decreto-Regulamentar nº 1/2021. B.O. da República de Cabo Verde. I Série-nº9 (29-01-2021) 207-212. Disponível em https://kiosk.incv.cv/1.1.9.3589/

Deloitte. (2022). *Cybersecurity in a post-pandemic world: A focus on financial services*. Disponível em https://www2.deloitte.com/cn/en/pages/financial-services/articles/financial-services-cybersecurity-global-organizations.html

Devoteam Cyber Trust (n.d.). *ISO 27001*. Disponível em: https://www.27001.pt/

EIOPA. (2019). *Cyber risk for insurers: challenges and opportunities.* Publications Office of the European Union. Disponível em https://register.eiopa.europa.eu/Publications/Reports/EIOPA_Cyber%20risk%20for%20insurers_Sept2019.pdf

Elliot, J. & Jenkinson, N. (2020). O risco cibernético é a nova ameaça à estabilidade financeira. *IMF Blog, Washington, DC.* Disponível em https://www.imf.org/pt/B*logs*/Articles/2020/12/07/blog-cyber-risk-is-the-new-threat-to-financial-stabil

ENISA (2023). *ENISA Threat Landscape 2023*. ENISA – European Union Agency for Cybersecurity. Disponível em https://doi.org/10.2824/782573

Ferreira, A., Marton, F. & Perez, G. (2022). Cibersegurança em serviços: um estudo bibliométrico. *Revista dos Mestrados Profissionais*, *11* (2), 174-189. Disponível em https://www.researchgate.net/publication/366420505_Ciberseguranca_em_Servicos_Um_Estudo_Bibliometrico

Governo de Cabo Verde. (2024a, 26 de janeiro). *Aprovada na generalidade a proposta de lei do Regime Jurídico dos Serviços Digitais e Comércio Eletrónico.* Disponível em https://www.governo.cv/aprovada-na-generalidade-a-proposta-de-lei-do-regime-juridico-dos-servicos-digitais-e-comercio-eletronico/

Governo de Cabo Verde. (2024b, 20 de junho). *Aprovada na especialidade a proposta de lei que regula o Regime Jurídico dos Serviços Digitais e Comércio Eletrónico"*. Disponível em https://www.governo.cv/aprovada-na-especialidade-a-proposta-de-lei-que-regula-o-regime-juridico-dos-servicos-digitais-e-comercio-eletronico/

Gulyas, O., & Kiss, G. (2023). Impact of cyber-Attacks on the financial institutions. *Procedia Computer Science*, *219*, 84–90. Disponível em https://doi.org/10.1016/j.procs.2023.01.267

Hill, M. & Hill, A. (2009). *Investigação por Questionário.* Lisboa, Portugal: Edições Sílabo, Lda.

Hsu, C., Wang, T., & Lu, A. (2016). The impact of ISO 27001 certification on firm performance. *49th Hawaii International Conference on System Sciences*, *2016-March*, 4842–4848. Disponível em https://ieeexplore.ieee.org/document/7427787

Huang, H. & Xu, C. (2000). *Financial Institutions, Financial Contagion, and Financial Crises.* (IMF Working Paper nº WP/00/92). Disponível em https://www.imf.org/external/pubs/ft/wp/2000/wp0092.pdf

IsecT Ltd. (n.d.). *ISO/IEC 27001 Security*. Retrieved from https://www.iso27001security.com/html/27001.html

ITU. (2021). *Global Cybersecurity Index 2020*. *International Telecommunication Union.* Disponível em https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Kellermann, T., & Murphy, R. (2020). *Modern Bank Heists 3.0.* VMware Carbon Black, Palo Alto, USA. Disponível em https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-modern-bank-heists-2020.pdf

Kosling, K. (2024, 13 de Março). *ISO 27001:2022 Annex A Controls Explained* [Web log post]. Disponível em https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained

Lei nº 133/V/2001. B.O. da República de Cabo Verde. I Série-nº2 (22-01-2001) 31-41

Lei nº 41/VIII/2013. B.O. da República de Cabo Verde. I Série-nº48 (17-09-2013) 1214-1217

Lei nº 8/IX/2017. B.O. da República de Cabo Verde. I Série-nº13 (20-03-2017) 318-325

Leite, L., & Oliveira, E. (2020). Modelo de processo de identificação de riscos cibernéticos em uma Instituição Financeira: um estudo baseado no NIST cybersecurity framework. In Oliveira, E. (Org.). *Tópicos em Administração* (Vol.

28, ppp. 38-50). Belo Horizonte: Editora Poisson. Disponível em https://doi.org/10.36229/978-85-7042-209-5

Marconi, M. & Lakatos, E. (2003). *Fundamentos de Metodologia Científica.* São Paulo, Brasil: Editora Atlas S.A.

Martins, A. (2023, 31 de Janeiro). Cabo Verde terá este ano centro nacional de cibersegurança. *Expresso das Ilhas*. Disponível em https://expressodasilhas.cv/pais/2023/01/31/cabo-verde-tera-este-ano-centro-nacional-de-ciberseguranca/84186

Masoud, N., & Al-Utaibi, G. (2022). The determinants of cybersecurity risk disclosure in firms' financial reporting: Empirical evidence. *Research in Economics*, *76*(2), 131–140. Disponível em https://doi.org/10.1016/j.rie.2022.07.001

Ministério das Finanças. (2021). *Cabo Verde sobe 27 posições no índice global de cibersegurança.* Disponível em https://www.mf.gov.cv/-/cabo-verde-sobe-27-posi%C3%A7%C3%B5es-no-%C3%ADndice-global-de-ciberseguran%C3%A7a-itu-

NIST. (2012). *Guide for conducting risk assessments*. National Institute of Standards and Technology. Disponível em https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Pereira, A. (2004). *SPSS: Guia Prático de utilização.* Lisboa, Portugal: Edições Sílabo, Lda.

Pollmeier, S., Bongiovanni, I., & Slapničar, S. (2023). Designing a financial quantification model for cyber risk: A case study in a bank. *Safety Science, 159*. Disponível em https://doi.org/10.1016/j.ssci.2022.106022

Quivy, R. & Campenhoudt, L. (1998). *Manual de Investigação em Ciências Sociais*. Lisboa, Portugal: Gradiva.

Rádio Alfa CV. (2023, 07 de Novembro). *O Cibercrime em Cabo Verde* [VIdeo File]. Disponível em https://www.youtube.com/watch?v=YKhwT_twVz0&t=5698s

Resolução nº 21/2016. B.O. da República de Cabo Verde. I Série-nº14 (07-03-2016) 531-549

Silva, G., & Ferrari, L. (2023). Ataques cibernéticos: a metáfora de guerra em ciências da computação. *Signo*, *48*(91), 31–41. Disponível em https://doi.org/10.17058/signo.v48i91.17937

US Government Accountability Office. (2018). *Weapon Systems Cybersecurity*. Disponível em https://www.gao.gov/products/gao-19-128

World Economic Forum (2016). *Understanding Systemic Cyber Risk*. Disponível em https://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf

Yin, R. (2010). *Estudo de Caso: Planejamento e Métodos*. Porto Alegre, Brasil: Artmed Editora S.A.

APÊNDICE A: GUIÃO E1: DEPARTAMENTO INFORMÁTICA, COMUNICAÇÃO E SEGURANÇA

- **Introdução**
  - Entrevista em português
  - Agradecer disponibilidade
  - Breve apresentação pessoal e objetivo da dissertação
  - Solicitação de consentimento para a gravação da entrevista
  - Confidencialidade de dados e informações para fins exclusivamente académicos
  - Objetivo da entrevista
- **História e Atualidade**
  1. Como descreveria a posição atual da CECV no mercado financeiro de Cabo Verde?
  2. Quais os principais serviços e produtos oferecidos pela CECV e como a tecnologia (internet e digitalização) desempenha um papel nessas ofertas?
- **Questões Gerais sobre Cibersegurança**
  3. Como descreveria a atual postura de cibersegurança da CECV? (Papel da segurança da informação na estratégia da instituição)
  4. Quais os principais objetivos e prioridades do departamento de Informática, Comunicação e Segurança em matéria de cibersegurança?
- **Políticas e Estratégias**
  5. Quais as principais estratégias de mitigação de riscos cibernéticos atualmente implementadas pela CECV? A CECV tem alguma parceria com outras entidades (pp.e. ARME/NOSi…)?
  6. Poderia descrever as medidas de segurança cibernética específicas que a CECV utiliza para proteger os seus sistemas e dados, e os dados dos clientes?
  7. Quais políticas de cibersegurança (regulamentos, documentos escritos, …) estão em vigor na CECV? Como são implementadas e monitorizadas?

8. A instituição possui um plano de resposta a incidentes cibernéticos? De uma forma geral, quais os procedimentos de deteção e resposta a incidentes de cibersegurança adotadas pela CECV?
9. Quais foram as principais medidas implementadas durante e após a pandemia para garantir a cibersegurança?

- **Capacitação e Sensibilização**

10. A CECV tem o hábito de promover ações de sensibilização e capacitação em matéria de cibersegurança aos funcionários? E aos clientes? Com que frequência são realizadas essas ações?

- **Desafios e vulnerabilidades**

11. Quais os principais desafios que a CECV enfrenta em termos de cibersegurança?
12. A CECV já sofreu algum incidente cibernético de alguma significância? Se sim, como foi a resposta?
13. Quais são as maiores vulnerabilidades da CECV, em termos de cibersegurança?
14. (Opcional). Vários autores consideram o RH o ativo mais vulnerável das instituições. Concorda com a afirmação?

- **Tecnologias e Investimentos**

15. Que tecnologias e ferramentas de cibersegurança o banco utiliza atualmente? Possui algum software/mecanismo de vigilância 24/7do ciberespaço?
16. A CECV tem um repositório ou sistema que regista e armazena o número de tentativas de ciberataques?
17. Quais os principais investimentos feitos pela CECV por forma a aumentar a robustez dos sistemas e a resiliência da instituição? Existem planos para investimentos futuros? A CECV tem um orçamento dedicado à cibersegurança?
18. Considera a aplicação CaixaNet (*mobile banking*) segura? Como é que garantem a sua segurança?

- **Certificação ISO 27001**

19. A CECV foi o 1º banco certificado pela ISO 27001. Como foi esse processo de obtenção do certificado ISO 27001? Quais foram os principais desafios?
20. Consegue detalhar os custos do processo de certificação? (Incluindo auditorias, formação e outras medidas implementadas… total de custos)

21. Quais os principais benefícios trazidos pela certificação ISO 27001 para a CECV, nomeadamente em matéria de cibersegurança? A certificação ISO 27001 teve impacto na confiança de clientes e parceiros/investidores?
22. Sabendo que foram alvo de auditoria para efeitos da recertificação da ISO 27001 recentemente, sabe se o resultado foi satisfatório? Como preparam para a auditoria? Alem de auditorias para ISO 27001, a CECV realiza outras auditorias em matéria de cibersegurança? Se sim, com que frequência?

- **Avaliação e Melhoria contínua**

23. Considera eficazes as estratégias de mitigação de riscos cibernéticos da CECV?
24. Que melhorias acredita serem necessárias nas estratégias de mitigação atuais?

- **Futuro da cibersegurança**

25. Quais são as suas expetativas para o futuro da cibersegurança na CECV e no mercado interbancário de Cabo Verde?

- **Análise documental**

26. Quais os principais dados e documentos que podem ser fornecidos para análise?
    - Relatórios de auditorias internas e externas
    - Plano de resposta a incidentes, Relatório de incidentes e relatório de avaliação pós-incidentes (se existentes)
    - Políticas, procedimentos e documentações internas de segurança

- **Encerramento**

27. Há mais algum aspeto relativo às estratégias de mitigação de riscos cibernéticos que queira destacar ou acrescentar?

- **Considerações Finais**
    - Agradecimentos, reiterar a importância da contribuição
    - Possibilidade de agendar entrevistas com administradores de rede
    - Confirmar próximos passos, nomeadamente sobre aplicação de questionários
    - Oferecer documento da tese após conclusão do estudo

APÊNDICE B: GUIÃO E2: ADMINISTRADORES DE REDE

- **Introdução**
  - Entrevista em português
  - Agradecer disponibilidade
  - Breve apresentação pessoal e objetivo da dissertação
  - Solicitação de consentimento para a gravação da entrevista
  - Confidencialidade de dados e informações para fins exclusivamente académicos
  - Objetivo da entrevista
- **Contexto Pessoal**
  1. Pode falar um pouco sobre a sua formação e experiência profissional?
  2. Qual a sua função na CECV? Há quanto tempo é administrador de rede?
- **Infraestrutura de Rede e Segurança**
  3. Podes descrever a infraestrutura de rede atual do banco?
  4. Quais são as principais medidas de segurança implementadas para proteger a rede da CECV?
- **Gestão de Incidentes Cibernéticos**
  5. Segundo informações já obtidas, a CECV nunca foi alvo de um ataque cibernético significativo, certo? Caso aconteça, quais são as principais etapas de resposta a esses incidentes? (Caso for possível responder, tendo em conta a confidencialidade)
  6. Como são tratadas as ameaças cibernéticas que ocorrem frequentemente?
- **Políticas e Protocolos de Segurança**
  7. Quais são as políticas e os protocolos de segurança cibernética mais importantes em vigor na CECV?

- **Formação e Sensibilização**

8. Recebe formação e capacitação em matéria de cibersegurança por parte da CECV? Se sim, com que frequência?
9. Acredita que os funcionários da CECV estão bem preparados para identificar e responder a ameaças cibernéticas?

- **Tecnologias e Ferramentas de Segurança**

10. Quais ferramentas e tecnologias de segurança cibernética mais utiliza no desempenho das suas funções? Como contribuem para a deteção e mitigação de riscos cibernéticos?

- **Certificação ISO 27001**

11. A CECV é o único banco de Cabo Verde certificado pela ISO 27001. Reconhece os benefícios trazidos pela ISO 27001 à CECV?
12. Qual a influência da ISO 27001 no desempenho das suas funções?

- **Desafios e melhorias**

13. Quais os maiores desafios enfrentados na proteção da rede contra ciberataques?
14. Quais incidentes acredita serem as maiores ameaças à rede da CECV, enquanto infraestrutura crítica do país?
15. Quais áreas dentro da CECV acredita merecerem mais atenção ou melhorias nas estratégias de segurança cibernética do banco, nomeadamente investimentos?

- **Avaliação das Estratégias de Mitigação**

16. Considera a rede da CECV robusta? A instituição tem uma boa capacidade de resiliência? (capacidade de continuar a operar serviços mínimos, mesmo após um incidente cibernético)
17. Considera eficazes as estratégias de mitigação de riscos cibernéticos da CECV?

- **Considerações Finais**

18. Há algo que gostaria de acrescentar sobre a cibersegurança em torno da CECV e no desempenho das suas funções?

- **Conclusão**

- Agradecimentos, reiterar a importância da contribuição
- Oferecer documento da tese após conclusão

APÊNDICE C: TRANSCRIÇÃO DA ENTREVISTA E1

- **História e Atualidade**

1. **Como descreveria a posição atual da CECV no mercado financeiro de Cabo Verde?**

R(I1): Neste momento é o 2º maior banco de Cabo Verde em termos de volume de negócio, clientes, créditos e depósitos.

2. **Quais os principais serviços e produtos oferecidos pela CECV e como a tecnologia (internet e digitalização) desempenha um papel nessas ofertas?**

R(I1): Em Cabo Verde os bancos são muito equiparados em termos de produtos e serviços oferecidos, não há muita diferenciação entre um banco e outro. Basicamente são serviços de crédito, depósitos, cartões e intermediação. A CECV há 8 anos que tem apostado fortemente na transformação digital, nomeadamente na disrupção da dependência de fornecedores externos (principalmente consultores portugueses): aposta no desenvolvimento interno com uma equipa formada há 4 anos, aposta na transformação de processos, nomeadamente mudança da mentalidade das pessoas, por forma a criar ferramentas que permitem mudar o banco no sentido de serem menos morosos e conservadores. Por exemplo, mudança de *workflow* de processos: redução de tarefas feitas em papéis através de uma ferramenta que ainda está numa fase prematura, que permite executar tarefas lentos e morosos que eram feitas em papéis e agora serão feitas digitalmente, por exemplo: antigamente um cliente de Santo Antão que queria pedir um crédito teria que enviar o processo por correio para a cidade da Praia, depois o comité de crédito reunia 1 vez por semana para fazer a análise dos créditos. Atualmente, a CECV tem uma plataforma de gestão documental desenvolvida por técnicos internos em que os pedidos são feitos nessa plataforma e a decisão é enviada diretamente para os tomadores de decisão, reduzindo drasticamente o tempo total do processo. Com isso há uma redução de +/-90.000 folhas de papel por ano. O processo ainda não é 100% digital pois há sempre um momento em que o cliente terá que deslocar-se ao balcão para assinar o contrato.

- **Questões Gerais sobre Cibersegurança**

3. **Como descreveria a atual postura de cibersegurança da CECV? (Papel da segurança da informação na estratégia da instituição)**

R(I1): A CECV, desde 2009, iniciou um processo de auditoria complexo de segurança de informação, culminando em 2012 com a certificação ISO 27001. A CECV é o único banco em Cabo Verde certificado com a ISO 27001 de segurança de informação. Desde essa altura, a CECV tem montado um processo de auditoria regular: fazemos 4 auditorias internas e 2 auditorias externas, por ano. Uma vez por ano a entidade certificadora da ISO 27001, Bureau Veritas, faz o processo de acompanhamento (*follow up*) de como tem sido o tratamento da segurança de informação dentro do banco. Terminou agora em início de Julho o último processo de acompanhamento e no próximo ano de 2025 será um novo processo de recertificação. Esta questão tem permitido à CECV estar um pouco na linha da frente no que diz respeito à segurança: na parte da segurança física, eletrónica, avaliação do plano de continuidade negócios, investimentos tecnológicos e formação das pessoas… passa um pouco pela mudança de paradigma drástica desde que iniciamos este processo. Portanto, é uma situação que nós temos muito bem montada, muito madura e que anualmente fazemos sempre o acompanhamento através de relatórios de auditoria, "*confining*", recursos a consultores externos, técnicos internos que diariamente lidam e dão sequência e seguimento a aquilo que os nossos auditores e consultores sugerem.

4. **Quais os principais objetivos e prioridades do departamento de Informática, Comunicação e Segurança em matéria de cibersegurança?**

R(I1): A certificação ISO 27001 tem um scope/âmbito que é essencialmente garantir a segurança da informação dos nossos clientes, tudo o que são ferramentas, tecnologias, processos que nós temos no banco que envolve informações dos clientes está debaixo deste "chapéu" onde se procura garantir que os nossos dados e os dados dos nossos clientes nunca sejam comprometidos.

- **Políticas e Estratégias**

5. **Quais as principais estratégias de mitigação de riscos cibernéticos atualmente implementadas pela CECV? A CECV tem alguma parceria com outras entidades (pp.e. ARME/NOSi…)?**

R(I1): Muito por força da nossa certificação ISO 27001, nós temos mantido a logica de procurar estar um passo a frente em relação a aquilo que são as preocupações em termos de segurança, desde logo na modernização do nosso parque informático, tanto em termos de redes como em termos de tecnologias em uso, equipamentos da linha da frente que estejam em *compliance* com aquilo que são as boas práticas internacionais, procurando sempre manter os nossos sistemas atualizados. Cada vez que fazemos uma auditoria avaliamos a maturidade dos sistemas e dos processos que temos montados, as próximas auditorias abarcam sempre outras áreas por forma a apanharmos o máximo possível dos nossos processos. Nós também temos montado um plano de continuidade de negócio em que fazemos testes bianuais: 2x por ano simulamos uma catástrofe que possa ter acontecido com o nosso *data center* e redirecionamos os nossos serviços para um *disaster recovery* que temos montado, que essencialmente recebe *backups* diários, recebe replicação em tempo real do nosso *core* bancário mas também todos os nossos sistemas que nós temos em termos de ambiente Windows e sistemas destruídos, e procuramos sempre testar esse plano para garantir que em caso de necessidade podemos facilmente, ou dentro daquilo que intendemos ser o tempo aceitável, redirecionar os nossos sistemas para um ambiente controlado (*disaster recovery*) que não é produtivo mas que nos garante um ambiente seguro suficiente para continuarmos a prestar os nossos serviços aos nossos clientes. Em termos de parceria, a CECV não tem nenhuma ligação com a rede do estado nem com nenhuma entidade local que em termos de parceria. A única coisa que os bancos têm é a conectividade com o banco central para a partilha de informações e também faz parte da rede Vinti4, rede de cartões da SISPP. Localmente não existe outra ligação.

6. **Poderia descrever as medidas de segurança cibernética específicas que a CECV utiliza para proteger os seus sistemas e dados, e os dados dos clientes?**

(Respondida ao longo de questões anteriores)

7. **Quais políticas de cibersegurança (regulamentos, documentos escritos, …) estão em vigor na CECV? Como são implementadas e monitorizadas?**

R(I1): Tem sim. O nosso sistema de gestão de informação é formado por 4 tipos de documentos: nós temos normas, manuais, procedimentos e registos. Este conjunto de documentos são atualizados anualmente e sempre que for necessário surgem novos

documentos. Esses documentos são geridos, aprovados e revistos por uma comissão de segurança que nós temos montado. Essa comissão é formada pelos administradores executivos, pelo auditor interno, pela direção de informática, por auditores externos e pelo consultor que trabalha connosco. Essa comissão reúne-se anualmente para avaliar KPI's (*Key Performance Indicators*), os projetos e também para fazer a revisão e atualização dos documentos. Esses documentos, depois de aprovados, são publicados na intranet onde todos os colaboradores têm acesso e podem ser consultados sempre que for necessário.

8. **A instituição possui um plano de resposta a incidentes cibernéticos? De uma forma geral, quais os procedimentos de deteção e resposta a incidentes de cibersegurança adotadas pela CECV?**

R(I1): A instituição possui um plano de continuidade de negócio e plano de recuperação de desastres. Fazemos testes regulares e simulações, nunca tivemos (ainda) uma situação real em que tivéssemos a necessidade de ativar o plano por força de um incidente.

9. **Quais foram as principais medidas implementadas durante e após a pandemia para garantir a cibersegurança?**

R(I1): Na CECV foi muito interessante este processo da pandemia. Um pouco antes da pandemia nós tivemos um processo de migração, por exemplo, do SWIFT (que é um sistema crítico para os bancos) que saiu do BCV (Banco Central de Cabo Verde) para a SISP (Sociedade Interbancária e Sistemas de Pagamentos). Ou seja, enquanto lá fora cada banco tem a sua conetividade à rede SWIFT, aqui em CV essa conetividade é partilhada por todos os bancos, ou seja, há uma entidade única e os bancos conectam à essa entidade. Na altura era BCV e passou para a SISPP. Neste processo de passagem para a SISP, a CECV optou, tendo em conta estas questões de transformação digital, por não ter impressão, ou seja, para cada mensagem SWIFT, cada transação que entra, cada transação que sai, é gerado um documento físico no papel. Este papel é um guião para que as pessoas dos departamentos estrangeiros processem os pedidos. Nós optamos, na altura da migração para a SISP, não ter papeis e passamos a ter apenas ficheiros em PDF. Este foi um ponto fundamental na questão da Covid. A partir que começou o confinamento tivemos a sorte de estar num processo de substituição de equipamentos, ou seja, o nosso parque de computadores estava já com alguma

degradação, já tinha chegado o momento de substituição destes equipamentos, e coincidiu que na altura da pandemia nos estávamos a concluir o processo de substituição destas máquinas, então muitos colaboradores dos serviços centrais passaram a ter portáteis, o que não tinham antes. A partir do momento em que houve o confinamento todo mundo dos serviços centrais foi para casa, apenas as agências que tiveram de manter em funcionamento, dividiu-se a equipa em 2: havia pessoas que iam segunda, quarta e sexta, havia pessoas que iam terça e quinta, em algumas agencias iam aos sábados. Mas nos serviços centrais todo mundo foi para casa. Montamos VPNs para que as pessoas pudessem trabalhar remotamente a partir de casa e, pelo menos no nosso departamento e com o nosso administrador, montamos reuniões diárias e semanais para irmos avaliando como é que as coisas estavam a funcionar. Tínhamos uma comissão de segurança que reunia mensalmente via Zoom, para avaliar como é que as coisas estavam, qual era o cenário, como é que estavam os projetos, quem é que tinha sido infetado, enfim, fomos fazendo estas reuniões regulares para garantir que as coisas funcionassem. Fiquei a saber por exemplo que a CECV foi o único banco que não teve ninguém nos serviços centrais a trabalhar, a maior parte dos bancos que não estavam preparados ou que não tinham condições para trabalhar remotamente tiveram que ir fisicamente para o escritório trabalhar. Nós fomos o único banco em que ninguém dos serviços centrais foi trabalhar presencialmente. Permitiu que trabalhássemos totalmente de casa. Houve, obviamente, colegas que não tinham condições para trabalhar em casa, ou porque não tinham internet, ou porque a própria natureza do seu trabalho era "desprezível", houve alguns colegas que passaram a fazer uma espécie de *lay-off*, ou seja, se estavam em casa, não estavam formalmente a trabalhar, mas continuaram sempre a receber os seus salários. Mas no grosso todos dos serviços centrais conseguiram trabalhar de casa tranquilamente.

- **Capacitação e Sensibilização**

10. **A CECV tem o hábito de promover ações de sensibilização e capacitação em matéria de cibersegurança aos funcionários? E aos clientes? Com que frequência são realizadas essas ações?**

R(I1): Nós temos por hábito fazer 2 coisas: sempre que um colaborador novo entra no banco, nós temos um processo chamado formação de integração, onde é lhe dado a conhecer quais são os normativos, como é que funciona os recursos humanos, como

funciona a área financeira, a área comercial… então nesse processo de integração de colaboradores que entram passou-se a incluir um sessão/manhã sobre a segurança de informação, em que o responsável do departamento de Segurança, Informação e Comunicação faz essa formação. Nessas formações, fazemos uma resenha daquilo que é a segurança de informação do banco, explicamos todos os procedimentos que nós temos, os documentos que existem e focalizamos muito na questão dos incidentes. Ou seja, reforçamos que sempre que ocorra algo fora do comum como é que deve ser reportado e, quando for reportado, como é que é feito o tratamento. E, a partir do ano passado, 2 vezes por ano, o responsável de segurança tem estado a fazer sessões com todos os colaboradores remotamente, via Teams, onde faz-se um reforço de como é que a instituição está em termos de segurança de informação, quais são os documentos mais relevantes, quais são os cuidados que nós devemos ter e como é que devemos comportar durante um cenário ou uma situação de stress, ataques ou incidentes. E também fazemos, via um canal que nós temos internamente no Outlook, que é o Comunica Comigo, onde regularmente fazemos uma espécie de um "tema da semana" onde é falado sobre cartões, sobre crédito… é falado sobre vários temas, mas também têm dias em que são exclusivos apenas para a segurança, onde nós falamos de que cuidados que nós devemos ter, como é que as coisas devem ser tratadas, muito focado no *phishing* e no *Ransomware*, explicar que nunca devem aceder ou abrir um email em que o remetente é desconhecido e que devem sempre encaminhar essas duvidas para a área da informática para nós avaliarmos como é que devem se comportar. Em relação aos clientes, nós temos feito algumas ações que são basicamente publicações que nós fazemos no nosso site, nos canais facebook e youtube, mas também por email costumamos fazer alertas aos clientes sobre os cuidados que devem ter com os seus códigos de acesso à *internet banking*, que o banco nunca está a pedir essas informações e que devem ter o cuidado de nunca responder. No passado, já houve muitos casos de ataques de *phishing* com clientes a serem afetados, mas desde que nós montamos o nosso novo *internet banking* passamos a usar o *one time password* e pronto estancou-se ali os ataques de *phishing*, mas continuamos sempre a fazer alertas por email aos clientes, publicações no nosso site e também nos canais digitais que temos.

- **Desafios e vulnerabilidades**

11. **Quais os principais desafios que a CECV enfrenta em termos de cibersegurança?**

R(I1): Como toda a instituição que esteja no mercado com conetividade com clientes, os desafios são diários e constantes. Ou seja, nós temos procurado acima de tudo manter os nossos sistemas completamente atualizados em relação a aquilo que são as boas práticas e as recomendações em termos de segurança. Nós procuramos, muito também por força da ISO 27001 e das auditorias que nós fazemos, regularmente nós estamos sempre a dar um passo a frente para estar mais atualizado possível e tentar criar ferramentas para permitir que os nossos clientes nunca são afetados. Em relação aos colaboradores, por exemplo, nós estamos neste processo que iniciamos em janeiro de *multifactor authenticator*, ou seja, qualquer login feito no *office* 365, ele vai obrigar-te a confirmar a tua identidade num canal alternativo. Também temos feito bloqueios a qualquer acesso de qualquer colaborador do banco que esteja fora de CV, isto é, os colaboradores nunca podem aceder fora de Cabo Verde sem que avise primeiro à Informática para ativar esse acesso. Portanto nós também temos tido essa preocupação. Fizemos um projeto muito grande que começou mais ou menos na pandemia, que foi um upgrade do nosso parque informático em termos de rede e network, ou seja, elevamos o nível da nossa arquitetura de rede para estar mais em *compliance* com o que são as boas práticas, tínhamos equipamentos muito antigos e neste momento temos equipamentos que estão na linha da frente em termos de daquilo que são as boas práticas em termos de segurança.

12. **A CECV já sofreu algum incidente cibernético de alguma significância? Se sim, como foi a resposta?**

R(I1): A instituição não sofreu até agora ataques de grande dimensão. Apenas faz testes regulares e simulações.

13. **Quais são as maiores vulnerabilidades da CECV, em termos de cibersegurança?**

R(I1): O maior desafio que nós temos, eu costumo dizer que são os “30 centímetros”, que é a distância entre o computador e a pessoa. Qualquer colaborador é sempre um vetor de possível ataque. Nós procuramos sempre com as formações e com as alertas

que nós fazemos para que estejam sempre atentos para evitar situações que possam colocar em risco a situação do banco. Tivemos uma situação muito interessante da última auditoria que agora acabou, o auditor externo quando cá esteve não foi visitar o *data center*, não foi às salas técnicas… fez uma coisa completamente diferente do que nós estávamos à espera: focou essencialmente nas pessoas. Foi a sala de todos os colaboradores verificar o caixote de lixo se encontrava documentos e teve ainda a capacidade de ir ao caixote de lixo fora do banco verificar os sacos que as senhoras da limpeza levaram para ver se existiam informações comprometedoras. Nós reunimos com as senhoras e dissemos "minha sra., olha, quando você for fazer a limpeza de uma sala, se encontrar um papel no caixote de lixo não limpe, deixe lá. Se a pessoa reclamar, que venha falar com o departamento de segurança para lhe explicar o porquê". Disponibilizar destruidores de papel em todas as salas e sítios públicos e evitar ao máximo as impressões, mas o cabo-verdiano é muito difícil nessas coisas. Nós temos pessoas que preferem imprimir para picar e depois colocar no lixo. É complicado. Há muitas pessoas que têm pedido impressoras nas suas salas, mas temos evitado isso. Tem gerado muito conflito, mas muitas vezes é por aí que nós temos que fazer. Outra coisa muito interessante que nós já iniciamos é a utilização da assinatura digital. Há muitos pedidos de extratos, principalmente nesta altura de férias e em que os miúdos vão para a universidade, então já montamos no nosso departamento a modalidade de extratos assinados digitalmente em *pdf* para se evitar as impressões. Ou seja, sempre que o cliente solicita um extrato com urgência, enviamos um extrato por *pdf* assinado por digital.

14. **(Opcional). Vários autores consideram o RH o ativo mais vulnerável das instituições. Concorda com a afirmação?**

(Respondido na questão anterior)

- **Tecnologias e Investimentos**

15. **Que tecnologias e ferramentas de cibersegurança o banco utiliza atualmente? Possui algum software/mecanismo de vigilância 24/7 do ciberespaço?**

R(I1): Bom, aqui não posso entrar em detalhes. (devido a confidencialidade). Nós temos ferramentas de monitorização que nós monitorizamos toda as redes das agências do banco, monitorizamos a conetividade, a"…", o CPU, a temperatura, a humidade… nós

temos ferramentas de login que armazenamos os *logs* e unificamos todos os *logs* numa ferramenta que é possível monitorizar para nós controlarmos e perceber como é que as coisas estão a funcionar… temos ferramentas de backups e de replicação em tempo real do core bancário e dos sistemas bancários. E também temos um centro de monitorização 24/24 com vigilantes que monitorizam tudo o que sejam videovigilância, intrusão, incêndio e controlo de acesso. E qualquer "alarmisse" que ocorra, qualquer situação que exista eles reportam automaticamente para o responsável de segurança e depois há um processo que é seguido naturalmente para dar sequência a estas alarmísticas.

16. **A CECV tem um repositório ou sistema que regista e armazena o número de tentativas de ciberataques?**

R(I1): Existe o sistema de logins que regista e reporta tudo isto, e nós depois monitorizamos e fazemos as nossas correções.

17. **Quais os principais investimentos feitos pela CECV por forma a aumentar a robustez dos sistemas e a resiliência da instituição? Existem planos para investimentos futuros? A CECV tem um orçamento dedicado à cibersegurança?**

R(I1): Sim, nós fazemos isso sempre. Fizemos isso recentemente com um investimento no nosso parque em termos de arquitetura de rede, mas estamos constantemente a fazer novos investimentos para melhorar o que nós temos: seja em termos de conetividade para termos largura de bandas mais fiáveis, seja em termos de melhorar tudo que seja a nossa conetividade com as agências e com os serviços que oferecemos. Anualmente temos um plano de investimentos que nós desenhamos e vamos seguindo para a melhoria dos nossos serviços.

18. **Considera a aplicação CaixaNet (mobile banking) segura? Como é que garantem a sua segurança?**

R(I1): Sim. Portanto é uma solução que foi montada e desenhada por pessoas externas, o portal tem certificado digital, fazemos auditorias regulares de *pentest* (testes de penetração) para garantir que não há falhas operacionais, está montada sobre um sistema de virtualização, portanto, é possível fazer melhorias de capacidade conforme for necessário e é uma solução sempre monitorizada e que é feita auditorias regulares para garantir que está em *compliance*.

- **Certificação ISO 27001**

19. **A CECV foi o 1º banco certificado pela ISO 27001. Como foi esse processo de obtenção do certificado ISO 27001? Quais foram os principais desafios?**

R(I1): O processo começou na altura da minha entrada para o banco (2008). Nesta altura havia um departamento de auditoria interna, mas não tinha o trabalho de auditoria informática, então esse processo começou comigo. A partir do momento que iniciamos este processo de auditoria, constatamos um conjunto de situações que precisavam de ser melhoradas, ou seja, as auditorias mostravam que para além dos investimentos em tecnologias e equipamentos faltava ainda muito investimentos em termos de processos, normativos, reengenharia de processos. Então quando nos iniciamos este processo de auditoria, que demorou 4 anos, fomos fazendo auditorias regulares, monitorizando sistemas, melhorando as coisas até chegar a um ponto em que sentíamos que de facto estávamos estáveis. Aí propusemos "porque não dar um salto ainda maior e tentar partir para uma certificação?". Aí sim contactamos os nossos consultores e auditores externos que sugeriram a Bureau Veritas e pronto, seguimos o guião da ISO 27001 em termos de documentação, o que é que nós tínhamos de ter em termos de boas práticas, em termos de processos, procedimentos, normativos… quando fizemos isso tudo, chamamos a Bureau Veritas e vieram constatar se estávamos ou não a cumprir com aquilo que nós tínhamos definido. E pronto, foi logo a partida, tivemos uma auditoria limpa, sem nenhuma contrariedade, e passamos logo a ser um banco certificado. Muito fruto dos investimentos feitos durante os 4 anos. Agora, o que é natural é que trouxe muitas vantagens para o banco em termos dos nossos processos melhorarem imenso, mas também trouxe muitos desafios porque tínhamos pessoas que estavam habituadas a fazer as coisas de uma maneira e agora tinham de fazer de outra maneira. Desde logo, por exemplo, pedidos de acesso, revisão de acessos, ferramentas de *ticketing*… até então as pessoas ligavam para a informática para fazer um pedido, a informática atuava conforme "…", agora não, é preciso de um ticket onde você tem que justificar, de o que é que precisa, quem fez, quando é que fez, quanto é que demorou… montagem KPIs, com indicadores, mostrar como é que as coisas a estavam a ser feitas, o que é que temos estipulado como razoável, o que é que foi atingido, se estavam ou não correto, enfim... tudo isto foi um desafio e tem sido um desafio enorme que diariamente temos estado a lidar com isso.

20. **Consegue detalhar os custos do processo de certificação? (Incluindo auditorias, formação e outras medidas implementadas… total de custos)**

R(I1): Muito difícil, não consigo quantificar. Foram custos enormes desde a contratação de consultores externos, de auditorias, das viagens, dos investimentos que foram feitos, da documentação, enfim… Colaborador foi a Portugal fazer uma formação de Lead Implementer da ISO 27001… Não consigo quantificar um valor.

21. **Quais os principais benefícios trazidos pela certificação ISO 27001 para a CECV, nomeadamente em matéria de cibersegurança? A certificação ISO 27001 teve impacto na confiança de clientes e parceiros/investidores?**

R(I1): Obviamente, a partir do momento que nós passamos a ser o único banco certificado com ISO 27001, tivemos que usar essa bandeira para provar aos nossos clientes que nós de facto estamos diferenciados em relação aos nossos concorrentes.

22. **Sabendo que foram alvo de auditoria para efeitos da recertificação da ISO 27001 recentemente, sabe se o resultado foi satisfatório? Como preparam para a auditoria? Alem de auditorias para ISO 27001, a CECV realiza outras auditorias em matéria de cibersegurança? Se sim, com que frequência?**

R(I1): Sim. As auditorias são sempre momentos interessantes. Não existem instituições perfeitas, costuma-se dizer que existem 2 tipos de instituições: aquelas que estão a ser atacadas e aquelas que não sabem que estão a ser atacadas. Todas as auditorias geralmente encontram sempre *findings* que são categorizados em termos de oportunidade de melhoria, ou uma observação, ou uma não conformidade que pode ser menor ou maior. Felizmente nunca tivemos não conformidades maiores, mas na base daquilo que é feito no trabalho da auditoria encontramos sempre ganhamos para a instituição. Ou seja, sempre surgem situações em que nós, que estamos diariamente com a mão na massa, não temos a noção de que podemos fazer coisas diferentes, e a visão do auditor é extremamente importante nesse aspeto, ele mostra sempre "ok, você está a fazer isto assim, mas as boas praticas dizem que você pode fazer mais isto ou mais aquilo". Então sempre nestes aspetos que nós temos visto as auditorias, tem sido sempre muito bom porque permite-nos sempre melhorar muito a nossa instituição.

- **Avaliação e Melhoria contínua**

23. **Considera eficazes as estratégias de mitigação de riscos cibernéticos da CECV?**

R(I1): Sim.

24. **Que melhorias acredita serem necessárias nas estratégias de mitigação atuais?**

R(I1): Eu acredito que vai de acordo com aquilo que os auditores nos reforçam todos os anos, que são mais sessões de training, mais sessões de *awarness*, procurar fazer simulacros, inclusive nós temos uma proposta que ainda não avançamos que é *ethical hacking*, isto é, instalar um aplicativo interno e este aplicativo despoletar situações de potenciais fraudes ou potenciais riscos para ver se os colegas respondem ou não ou como é que eles reagem. Portanto, cenários do género eu acho que seria importante fazer-se, ou seja, mais formações, mais *awarness* e alguns simulacros anónimos para perceber se os utilizadores respondem ou não, se reagem ou não, se caem no isco e, conforme isso ocorrer, fazer mais ações para perceber como é que devem reagir em cenários do género.

- **Futuro da cibersegurança**

25. **Quais são as suas expetativas para o futuro da cibersegurança na CECV e no mercado interbancário de Cabo Verde?**

R(I1): É assim, a cibersegurança em CV, eu penso, se não se avançar para um CSIRT a nível nacional como existem lá fora em outros países, pelo menos devia-se avançar para um CSIRT financeiro. Ou seja, todos bancos terem um centro de monitorização que reporta para a área financeira situações que acontecem. Portanto, não existe em CV nada do género, não existe colaboração entre as instituições financeiras e algumas vezes nós percebemos que aconteceu algo, mas por não haver partilha e troca de informação não se consegue de certa forma avaliar se outras instituições do género também poderão estar vulneráveis lá onde falhou uma outra instituição. Portanto, tem de haver mais colaboração, está a ser difícil montar uma CSIRT nacional que alberga ou que centraliza informações de todas as instituições consideradas críticas, mas penso que pelo menos a área financeira devia avançar para algo do género para que possamos estar mais ativos e atentos a potenciais riscos. A área financeira merece uma atenção especial.

- **Análise documental**

26. **Quais os principais dados e documentos que podem ser fornecidos para análise? (Considerar comparação antes e depois da adoção da ISO 27001)**

R(1): Os documentos que nós temos são classificados, no âmbito da ISO 27001, de documentos de uso interno. É muito complicado fazer a partilha desses documentos para fora da instituição. Os relatórios e contas têm lá informações que podem ser uteis e estão disponíveis.

- **Encerramento**

27. **Há mais algum aspeto relativo às estratégias de mitigação de riscos cibernéticos que queira destacar ou acrescentar?**

R(I1): Não, é tudo.

APÊNDICE D: TRANSCRIÇÃO DA ENTREVISTA E2

- **Contexto Pessoal**

1. **Pode falar um pouco sobre a sua formação e experiência profissional?**

R(I2): Eu fiz a licenciatura na universidade do Minho (1988-2004) em Informática de Gestão, depois comecei a trabalhar em Lisboa na área de modelação de processos. Mas depois não estava a gostar muito e apareceu uma oportunidade de fazer um pós-graduação em Computação Gráfica, por acaso nunca cheguei a exercer esse curso que eu fiz de pós-graduação, que foi feito nos EUA durante 1 ano. Depois, tinha que decidir entre voltar para a Portugal e seguir carreira em Portugal ou voltar para Cabo Verde. Decidi regressar para Cabo Verde, entrei no NOSi e estive lá 5 anos a trabalhar no departamento de administração de sistemas, que é sobre sistemas operativos, DNS, DHCPs, emails, antivírus… Depois apareceu a oportunidade de trabalhar na CECV e então no final de 2011 entrei na CECV para o departamento de infraestruturas. A diferença é que agora na CECV, para além de sistemas, trabalho também na parte de redes e segurança. E pronto, até agora tenho estado muito a trabalhar nesta parte, sempre redes, sistemas e a parte de segurança também. Estamos a trabalhar muito na parte de segurança por causa das auditorias que temos tido todos os anos, também temos uma empresa que faz todos os anos um *assessment* na CECV, eles fazem um relatório enorme e nós temos que corrigir vários *findings* que eles descobrem e é isso. No ano passado decidi fazer outra pós-graduação em segurança informática na Uni-CV, terminou agora no mês de junho. Basicamente nós é que somos os responsáveis pela infraestrutura da CECV, parte de sistemas, redes e segurança.

2. **Qual a tua função na CECV? Há quanto tempo é administrador de rede?**

(Respondida na questão anterior)

- **Infraestrutura de Rede e Segurança**

3. **Podes descrever a infraestrutura de rede atual do banco?**

R(I3): Começando pelas *facilities:* temos um *data center inhouse*, no edifício sede com controlo biométrico na entrada e registo das entradas, para ter o registo de pessoas (quem e quando teve acesso) e controlar quem pode ter acesso ao *data center*. O *data center* tem controlo climático, portanto, temperatura, humidade e ar condicionado, para

além da monitorização de vídeo que é acompanhada 24/7 pela equipa de segurança física, e também de sistemas automáticos de estimação de incêndio. O *data center* principal é acompanhado por um *data center* de *disaster recovery* numa das agências na Praia, temos então uma ligação de fibra que utilizamos para fazer a replicação dos principais servidores para garantir a continuidade do negócio. No *data center*, em termos de equipamentos, temos equipamentos do sistema core bancário que é uma infraestrutura a parte, depois temos equipamentos de virtualização, uma vez que todas as outras aplicações e serviços são baseadas em máquinas virtuais. Temos também alguns servidores que obrigatoriamente têm de ser físicos: servidores de gestão de acessos e identidades, mas também servidores de suporte ao pessoal de segurança física, de vigilância, etc. Também temos os nossos equipamentos de rede, onde através das nossas operadoras, temos ligação para a internet, ligações para cada uma das agências e também ligação para nosso parceiro interbancário, que é o SISP, equivalente ao SISB em Portugal, que garante a presença da CECV no sistema financeiro nacional: SWIFT, vinti4, transferências interbancárias, Visa, etc. O nosso *home banking* é inhouse/interno, portanto, temos a disponibilização de serviços através da internet, o *home banking* e o *mobile banking*. Neste momento, seguindo as tendências o nosso email é na cloud através do Microsoft 365. Depois nos serviços de infraestruturas, temos os serviços típicos de suporte à rede como antivírus, manutenção de infraestruturas, gestão de *logs*, algumas aplicações a volta do negócio: gestão de créditos, gestão de operações, aplicações de comunicação com os clientes, avaliação de desempenho, gestão de projetos, etc. Basicamente, de forma resumida é esta a nossa infraestrutura.

4. **Quais são as principais medidas de segurança implementadas para proteger a rede da CECV?**

R(I3): Começando pela parte física, as principais medidas de segurança em termos dos equipamentos físicos são os equipamentos em *data center* que garantem as condições de funcionamento ótimo em termos de temperatura, redundância de energia, humidade, etc., controlo físico para não permitir acesso indevido e também a réplica no data *center recovery* para garantir a continuidade do negócio. Subindo de nível, a nível de virtualização e de equipamentos de rede, temos equipamentos redundantes, são sempre mais do que um equipamento para fazer uma certa função de infraestrutura. Depois a nível dos dados, os dados são guardados seguindo a regra de boas práticas que é o 3-2-

1: 3 cópias de dados em 2 meios diferentes e pelo menos 1 guardado em outro espaço físico. Essas cópias de dados são cópias para tapes e cópias para discos, depois uma dessas cópias fica no *disaster recovery*. Mais acima para as aplicações, neste momento estamos numa fase de sequencialmente migrar as aplicações web, que é a maior parte das aplicações, para *https* para que de um lado garantir a confidencialidade através da encriptação, mas também para garantir que do lado do utilizador da aplicação que está a interagir com um sistema fidedigno. Obviamente que as aplicações que estão disponíveis na internet para os clientes, já têm essa garantia, são todos *https* com certificados que dão essa garantia. Também, do lado dos utilizadores, tirando partido do "documento/departamento" de controle da Microsoft, que é o *default* da maior parte das organizações para a gestão de identidade, garantimos um controle apertado nas contas dos utilizadores, as passwords têm de ser alteradas, as *passwords* têm de ter um mínimo de carateres, têm de ter carateres especiais (números, algarismos minúsculos e maiúsculos) para garantir uma certa complexidade, e também na parte dos administradores de infraestruturas que têm um acesso mais privilegiado, esses controlos são mais apertados e restritos em relação ao tempo de vida das passwords, também o seu tamanho e a sua complexidade. Todos os registos, os logins dos utilizadores, são depois gravados para consulta posterior em caso de algum evento malicioso. Isto tudo são boas práticas que seguimos porque a CECV decidiu ser uma entidade certificada pela ISO 27001, que nos obriga a ter uma certa postura de segurança, sofremos auditorias internas do nosso parceiro de cibersegurança para preparar-nos então para auditorias formais do emissor do certificado que é feito anualmente.

- **Gestão de Incidentes Cibernéticos**

5. **Segundo informações já obtidas, a CECV nunca foi alvo de um ataque cibernético significativo, certo? Caso aconteça, quais são as principais etapas de resposta a esses incidentes?**

(Não respondida por ser confidencial)

6. **Como são tratadas as ameaças cibernéticas que ocorrem frequentemente?**

R(I2): Normalmente, o que acontece é que identificamos um ataque, é isolado o local que está a ser atacado e logo a seguir, em conjunto com uma empresa que temos parceria, nós fazemos uma investigação e tentamos resolver. Enquanto o processo não for resolvido, o local fica isolado. Se for um serviço bastante crítico, neste caso é feito

um encontro entre as partes de segurança que temos na CECV e tentamos repor o mais breve possível o sistema.

- **Políticas e Protocolos de Segurança**

7. **Quais são as políticas e protocolos de segurança cibernética mais importantes em vigor na CECV?**

(Não respondida por gestão de tempo e fora respondida na entrevista E1.)

- **Formação e Sensibilização**

8. **Recebe formação e capacitação em matéria de cibersegurança por parte da CECV? Se sim, com que frequência?**

R(I2): Normalmente não recebemos. Tentamos manter-nos sempre informados e acompanhando as novidades que há e, como temos uma empresa parceira da parte da área de segurança, há muita troca de informação e temos pequenas formações, mas não existe uma periodicidade fixa. É sempre que for necessário. Basicamente todos os anos há formações e ações de sensibilização/capacitação.

9. **Acredita que os funcionários da CECV estão bem preparados para identificar e responder a ameaças cibernéticas?**

R(I2): Foge um pouco da nossa área. Existe um gabinete mesmo que faz auditoria de sistemas de informação da CECV. (não respondida por estar fora do âmbito das funções dos entrevistados)

- **Tecnologias e Ferramentas de Segurança**

10. **Quais ferramentas e tecnologias de segurança cibernética mais utiliza no desempenho das suas funções? Como contribuem para a deteção e mitigação de riscos cibernéticos?**

R(I3): Para a cláusula disponibilidade, usamos uma aplicação que interage com o nosso sistema de virtualização e que consegue garantir-nos as operações de backup dos dados e a replicação, que é a copia dos dados do dia para o *data center disaster recovery*. Para intrusões, usamos *firewalls* de nova geração, com subscrição a servir-se de segurança onde aplicamos prevenção de intrusões, antivírus, controlo de aplicações e filtragem de endereços que os utilizadores podem aceder. Também, nos postos de trabalho, nos servidores, temos instalado antivírus que recebem atualizações de forma automática do

fabricante e os sistemas operativos dos utilizadores recebem *updates* regulares e de segurança dos fabricantes. Ainda no sistema de email que está delegado ao provedor de serviço na *cloud* tiram partido dos mecanismos de segurança que eles têm: antisspam, antimalware, antiphishing. Os nossos sistemas de email, completamos recentemente o trio de controlo de segurança de email que é o SPF, DKIM e DMARC para garantir a legitimidade dos emails enviados dos nossos sistemas. Na operação, no dia-a-dia, temos os sistemas de monitorização e também os sistemas de análise de *logs* que cada um dos equipamentos produzem.

- **Certificação ISO 27001**

11. **A CECV é o único banco de Cabo Verde certificado pela ISO 27001. Reconhece os benefícios trazidos pela ISO 27001 à CECV?**

(Respondida juntamente com a questão seguinte.)

12. **Qual a influência da ISO 27001 no desempenho das suas funções?**

R(I3): Traz benefícios claros. Primeiro para os nossos clientes, como disse anteriormente, não é uma imposição, a própria CECV decidiu buscar essa certificação para garantir aos clientes que a CECV está preocupada com a questão da cibersegurança e proteção de dados pessoais, portanto, há uma melhoria reputacional em frente aos nossos clientes, melhora a operação no dia a dia da CECV porque a certificação ISO 27001 não se cinge a parte tecnológica. Abrange por exemplo, a parte de *facilities* de *data center*, mas também desde recursos humanos, entrada e saída de pessoas, a forma como é feita o descarte de dados seja digital ou em suporte papel. E também de como os utilizadores comportam com dados pessoais dos clientes, ou por exemplo, a regra de mesa/secretária limpa onde os colaboradores não podem deixar documentos que podem conter dados confidenciais em cima da sua mesa de trabalho. Portanto, a ISO 27001 é mais do que tecnologia. Por fim, melhora o nosso desempenho de cibersegurança porque exige-nos uma iniciativa de melhoria continua, portanto sempre que conseguimos chegar a um patamar de configuração para melhor segurança de informação, a auditoria identifica no ano seguinte oportunidades de melhoria e então vamos tendo sempre essa postura de melhoria continua e atualizada com standard mundial. Resumidamente, é a reputação do banco do ponto de vista dos clientes, melhoria das operações do banco e melhoria do aspeto tecnológico.

- **Desafios e melhorias**

13. **Quais os maiores desafios enfrentados na proteção da rede contra ciberataques?**

(Respondida juntamente com a questão seguinte.)

14. **Quais incidentes acredita ser as maiores ameaças à rede da CECV, enquanto infraestrutura critica do país?**

R(I3): Os maiores desafios que nós enfrentamos, como qualquer outra organização e principalmente como uma organização financeira, é nessa recorrente do *Ransomware*. O vetor de entrada do *Ransomware* é muito difícil de controlar, mais de 90% dos *Ransomware* entram através do email em que o utilizador faz um clique num link qualquer, por isso é muito importante a parte de sensibilização dos trabalhadores, mas também a parte de proteção dos sistemas de email, essa é uma das preocupações que temos. A segunda preocupação que temos, é a migração sequencial de dados e aplicações para *cloud* que abre uma nova superfície de impacto que neste momento as políticas de segurança que nós utilizamos não cobrem esta nova realidade que é a *cloud*. E em terceiro lugar, diria que é a crescente complexidade no geral de toda a tecnologia de suporte ao digital que nos obriga, neste caso, o pessoal técnico a estar constantemente atualizado nas várias aplicações, nas várias ferramentas, mas também nos vários mecanismos de defesas de cada uma dessas novas soluções.

15. **Quais áreas dentro da CECV acredita merecerem mais atenção ou melhorias nas estratégias de segurança cibernética do banco, nomeadamente investimentos?**

R(I2): Primeiramente é o core business da CECV, é a área que temos maior preocupação, mas também a área do nosso *home banking*. Essas 2 áreas, tanto o core business como o *home banking*, são as áreas que mais devemos ter atenção porque é basicamente o motor da sustentabilidade de todo o negócio da CECV.

- **Avaliação das Estratégias de Mitigação**

16. **Considera a rede da CECV robusta? A instituição tem uma boa capacidade de resiliência? (capacidade de continuar a operar serviços mínimos, mesmo após um incidente cibernético)**

R(I3): Não podemos afirmar isso, mas esse é o ponto de chegada que apontamos todos os nossos esforços. Nunca conseguimos chegar a um ponto de perfeição, sempre que dás um passo aparece novos objetivos e novas oportunidades de melhoria.

17. **Considera eficazes as estratégias de mitigação de riscos cibernéticos da CECV?**

R(I3): Sim, tendo em conta que a instituição ainda não enfrentou nenhum ataque significativo.

- **Considerações Finais**

18. **Há algo que gostaria de acrescentar sobre a cibersegurança em torno da CECV e no desempenho das suas funções?**

R(I2) (I3): Não

APÊNDICE E: ANÁLISE DE CONTEÚDO DA ENTREVISTA E1

*Todas as respostas foram da autoria de I1

Categorias	
Subcategorias	**Unidades de Registo**
A. Contexto do mercado cabo-verdiano	
A.1 Posicionamento no mercado interbancário de Cabo Verde	Neste momento, é o 2º maior banco de Cabo Verde em termos de volume de negócio, clientes, crédito, depósitos. Em Cabo Verde, os bancos são muito equiparados em termos de produtos e serviços oferecidos. Não há muita diferenciação entre os bancos. Único banco em Cabo Verde certificado com a ISO 27001. Bancos em Cabo Verde partilham uma única conetividade à rede SWIFT, através da SISPP. A CECV não tem nenhuma ligação com a rede do Estado nem com nenhuma entidade local em termos de parceria. Os bancos têm conectividade com o banco central e fazem parte da rede Vinti4 (rede de cartões da SISP).
A.2 Cibersegurança no contexto nacional	Não existe em Cabo Verde um CSIRT. Não existe colaboração entre as instituições financeiras. Tem que haver mais colaboração. Não há partilha e troca de informações e por isso não se consegue aprender com acontecimentos passados e erros cometidos por outras instituições.
B. Estratégias de cibersegurança	
B.1 Infraestruturas, tecnologias e ferramentas existentes	Parque informático (rede e tecnologias) modernizado recentemente. Procuramos manter os sistemas sempre atualizados (estar o mais atualizado possível) Processo iniciado em janeiro de *multifactor authenticator* para os colaboradores. Implementação do *one-time password* para clientes no acesso à internet banking Aplicação CaixaNet montada e desenhada por pessoas externas.

	Aplicação e portal *home banking* com certificado digital. Portal criado sobre sistema de virtualização Utilização de assinatura digital. Temos ferramentas de monitorização para todas as redes das agências do banco. Monitorizamos a conetividade, o CPU, a temperatura, humidade… Temos ferramentas de logins que armazenamos e unificamos os *logs*. O sistema de logins regista e reporta as tentativas de acesso. Temos ferramentas de backups e de replicação em tempo real do core bancário e dos sistemas bancários. Temos um centro de monitorização 24/24 com vigilantes que monitoriza tudo o que seja videovigilância, intrusão, incêndio, e controlo de acesso. Temos um *data center*. Temos um *disaster recovery* montado que recebe backups diários e replicação em tempo real do nosso core bancário e todos os nossos sistemas. Garante um ambiente seguro o suficiente para continuar a prestar os nossos serviços.
B.2 Procedimentos de resposta e de proteção dos dados e produtos/serviços	Consideram-se eficazes as estratégias de mitigação de riscos cibernéticos da instituição Processo de auditorias regulares: 4 auditorias internas e 2 auditorias externas por ano. Monitorização e auditorias regulares de *pentest* ao serviço de *mobile banking* (CaixaNet) e ao portal. Uma vez por ano a Bureau Veritas faz o processo de acompanhamento de como tem sido o tratamento da segurança de informação dentro do banco. Acompanhamento anualmente através de relatórios de auditoria, "*confining*", recurso a consultores externos e existência de técnicos internos que lidam com as sugestões dos auditores e consultores. Nós temos um plano de continuidade de negócio Fazemos testes bianuais: 2x por ano simulamos uma catástrofe no nosso *data center*. A instituição possui um plano de recuperação de desastres. Bloqueio a qualquer acesso de qualquer colaborador do banco que esteja fora de Cabo

	Verde sem avisar ao departamento de Informática. Qualquer situação de alarme detetada pelo centro de monitorização é comunicada ao responsável de segurança da instituição que desencadeia o processo de resolução existente adequado. O departamento de Segurança, Informática e Comunicação monitora e faz as devidas correções a todas as situações detetadas pelo sistema de logins.
B.3 Políticas e normativos internos	Temos 4 tipos de documentos: normas, manuais, procedimentos e registos. São geridos, aprovados e revistos anualmente por uma comissão de segurança. Comissão de segurança é formada pelos administradores executivos, pelo auditor interno, pela direção de informática, por auditores externos e por consultores externos. Os documentos são publicados na intranet da instituição para todos os colaboradores terem acesso. Política de não impressão: evitar o máximo possível as impressões. Disponibilização de destruidores de papel em todas as salas.
B.4 Histórico de incidentes cibernéticos	No passado, já houve muitos casos de ataques de *phishing* com clientes a serem afetados na internet banking. A instituição não sofreu até agora ataques de grande dimensão. Apenas faz testes regulares e simulações. A instituição nunca teve uma situação real em que tivemos a necessidade de ativar o plano.
C. Certificação ISO 27001	
C.1 Principais benefícios e implicações resultantes da certificação ISO 27001	Único banco em Cabo Verde certificado com a ISO 27001 de segurança limpa de informação (reputação). Tem permitido à CECV estar um pouco na linha da frente no que diz respeito à segurança, na parte da segurança física, eletrónica, avaliação do plano de continuidade negócios, investimentos tecnológicos e formação das pessoas. A certificação ISO 27001 tem um scope/âmbito que é essencialmente garantir que os nossos

	dados e os dados dos nossos clientes nunca sejam comprometidos. Modernização do parque tecnológico, com equipamentos que estejam em *compliance* com aquilo que são as boas práticas internacionais. Melhorias nos nossos processos. Modo de provar aos clientes que a CECV está diferenciada em relação aos concorrentes. Impacto na confiança dos clientes e de investidores.
C.2 Custos, desafios e duração do processo de obtenção da certificação	A CECV desde 2008 iniciou um processo de auditoria complexo de segurança de informação, culminando em 2012 com a certificação ISO 27001. Demorou 4 anos (…). Foi uma auditoria limpa e conseguiu-se a certificação logo à partida Em 2008, havia um departamento de auditoria interna, mas não tinha o trabalho de auditoria informática. O processo passa um pouco pela mudança de paradigma drástica. Além de investimentos em tecnologias e equipamentos, eram necessários investimentos em termos de procedimentos, normativos, reengenharia de processos, boas práticas. Bureau Veritas: empresa responsável pela certificação. Houve desafios nomeadamente hábito das pessoas. Houve mudanças no modo de fazer coisas. Exemplos: pedidos de acesso, revisão de acessos, ferramentas de *ticketing*, montagem de KPI's (indicadores de performance). Não consigo quantificar os custos em valor. Foram custos enormes com: contratação de consultores externos, de auditorias, das viagens, dos investimentos que foram feitos, da documentação, formação *Lead Implementer* da ISO27001 para técnico específico do banco (em Portugal)
D. Cultura Organizacional e Capacitação	
D.1 Existência de ações de formação, sensibilização e desenvolvimento em matéria de cibersegurança	Existe um processo chamado formação de integração, destinado a novos colaboradores. É dado a conhecer os normativos, o funcionamento da instituição, etc. Há uma sessão destinada a segurança de informação. Desde o ano passado, 2x ao ano o responsável de segurança faz sessões online com os

	colaboradores sobre temas relacionados com a segurança de informação. Existe um programa "Comunica Comigo" transmitido através de um canal interno no Outlook, onde se faz uma espécie de "tema da semana", com dias exclusivos para a segurança. Aborda questões relacionadas com boas práticas de cibersegurança, com foco na *phishing* e *ransomware.* Em relação a clientes, faz-se publicações sobre alertas, cuidados e boas práticas de cibersegurança, nos canais da instituição (site, Facebook e Youtube), mas também por email.
D.2 Principais investimentos em cibersegurança	Modernização/upgrade recente do parque informático da instituição, em termos de tecnologias e arquitetura de rede. Melhoria de largura de bandas mais fiáveis. Aposta na mudança de mentalidade das pessoas Existência de plano de investimentos anual.
D.3 Principais vulnerabilidades, desafios e ameaças à instituição	Maior desafio são os "30 centímetros": distância entre o computador e o utilizador. Qualquer colaborado é sempre um vetor de possível ataque. Resistência dos colaboradores às mudanças, nomeadamente a não impressão. Conflitos gerados pela não disponibilização de impressoras em algumas salas de colaboradores.
D.4 Desafios trazidos pela Covid-19 e processo da digitalização	Há 8 anos a apostar forte na transformação digital Aposta na disrupção da dependência de fornecedores através da criação de uma equipa de desenvolvimento interno. Mudança de *workflow* de processos: redução de tarefas feitas em papéis. Desenvolvimento interno de uma plataforma de gestão documental, reduzindo o consumo de +/- 90.000 folhas de papel/ano. Processo de migração: passagem do SWIFT do Banco Central para o SISPP. Não impressão das mensagens SWIFT, passando a serem feitas através de ficheiros PDF. Disponibilização de computadores portáteis a alguns colaboradores de serviços centrais. A CECV foi o único banco em que todos dos serviços centrais foram trabalhar remotamente na altura do confinamento.

	Instalação de VPNs. Estabelecimento de reuniões de avaliação diárias e semanais. Existência de uma comissão de segurança que se reunia mensalmente para avaliar o estado. Alguns colaboradores colocados em "*lay-off*".
D.5 Feedbacks e Oportunidades de melhoria	Por não haver um CSIRT nacional, devia-se avançar para um CSIRT financeiro. Isto é, todos os bancos terem um centro de monitorização que reporta situações que acontecem na área financeira. A área financeira merece uma atenção especial. "Existem instituições que estão a ser atacadas e aquelas que não sabem que estão a ser atacadas" As auditorias encontram sempre *findings*, que são categorizados como oportunidades de melhoria, observação ou não conformidade (menor ou maior). Nunca tivemos não conformidades maiores. A visão do auditor é extremamente importante por nos permitir fazer coisas de forma diferente, de acordo com as boas práticas. As auditorias têm sido muito boas por nos permitir sempre melhorar a nossa instituição. Melhorias: mais ações de training, mais sessões de *awarness*, procurar fazer simulacros anónimos, mais formações. Há uma proposta que ainda não foi avançada, que é o *ethical hacking.*

APÊNDICE F: ANÁLISE DE CONTEÚDO DA ENTREVISTA E2

Subcategorias	Unidades de Registo
A. Perfil do Entrevistado	
A.1 Percurso acadêmico	(I2) Licenciatura na universidade do Minho em informática de gestão. (I2) Pós-graduação em computação gráfica, em EUA. (I2) Pós-graduação em segurança informática na Uni-CV.
A.2 Experiência profissional e funções atuais	(I2) Comecei a trabalhar em Lisboa na área de modelação de processos. (I2) Nunca trabalhei na área da pós-graduação em computação gráfica. (I2) Trabalhei no NOSi durante 5 anos no departamento de administração de sistemas. (I2) No final de 2011 entrei na CECV para o departamento de infraestruturas. (I2) Para além de sistemas, trabalho também na parte de redes e segurança.
B. Infraestrutura de Rede e Tecnologias de Segurança	
B.1 Descrição da infraestrutura de rede da instituição	(I3) *Facilities*: temos um *data center inhouse*, no edifício sede. (I3) O *data center* principal é acompanhado por um *data center* de *disaster recovery.* (I3) Réplica no *data center recovery* para garantir a continuidade. (I3) Em termos de equipamentos, temos equipamentos do sistema core bancário (…), equipamentos de virtualização. (I3) Servidores físicos: servidores de gestão de acessos e identidades, mas também servidores de suporte ao pessoal de segurança física, de vigilância, etc. (I3) Equipamentos de rede: ligação de fibra, ligação com cada agência, ligação com o parceiro interbancário (SISP). (I3) Serviços de suporte à rede: antivírus, manutenção de infraestruturas, gestão de *logs*, algumas aplicações a volta do negócio.

B.2 Tecnologias e Ferramentas de Segurança	(I3) *Data center* tem controlo biométrico na entrada e registo das entradas (quem e quando teve acesso) e controlar quem pode ter acesso. (I3) *Data center* tem controlo climático, portanto, temperatura, humidade e ar condicionado. (I3) Sistema de monitorização de vídeo que é acompanhada 24/7 pela equipa de segurança física. (I3) Sistemas automáticos de estimação de incêndio. (I3) Aplicações disponibilizadas aos clientes na internet em *https* e certificados de garantia de segurança. (I3) Para a cláusula disponibilidade, usamos uma aplicação que interage com o nosso sistema de virtualização e que consegue garantir-nos as operações de backup e replicação dos dados. (I3) Para intrusões, usamos *firewalls* de nova geração (prevenção de intrusões, antivírus, controlo de aplicações e filtragem de endereços). (I3) Nos postos de trabalho, nos servidores, temos instalado antivírus que recebem atualizações de forma automática. (I3) Sistemas de análise de *logs* produzido por cada um dos equipamentos.
C. Processos e Procedimentos	
C.1 Procedimentos, medidas e políticas de proteção de sistemas e dados	(I3) Replicação dos principais servidores para garantir a continuidade do negócio (*data center recovery*) (I3) Equipamentos redundantes: são sempre mais do que um equipamento para fazer uma certa função de infraestrutura (I3) Dados guardados seguindo a regra 3-2-1: 3 cópias de dados em 2 meios diferentes e pelo menos 1 guardado em outro espaço físico (I3) Cópias para tapes e cópias para discos (I3) Processo de migração das aplicações web para *https* (I3) Controlo apertado nas contas dos utilizadores: *passwords* têm de ser alteradas, *passwords* com um mínimo de carateres e com carateres especiais, complexos (I3) Controlos mais apertados e restritos para os administradores de infraestruturas que têm acesso mais privilegiado

	(I3) Todos os registos e logins dos utilizadores são depois gravados para consulta posterior (I3) Auditorias internas do nosso parceiro de cibersegurança para preparar-nos para auditorias formais do emissor do certificado, anualmente (I2) Temos uma empresa parceira que todos os anos faz um *assessment* na CECV e temos que corrigir os vários *findings* indicados (I3) Sistemas operativos dos utilizadores recebem *updates* regulares e de segurança (I3) Sistema de email delegado ao provedor de serviço na *cloud* com mecanismos de segurança: *antisspam*, *antimalware*, *antiphishing* (I3) Trio de controlo de segurança de email que é o SPF, DKIM e DMARC (I3) Regra de mesa/secretária limpa: não deixar documentos que podem conter dados confidenciais em cima da mesa de trabalho (I2) Quando há uma ameaça cibernética, identificamos o ataque, é isolado o local atacado e logo a seguir, em conjunto com uma empresa que temos parceria, nós fazemos uma investigação e tentamos resolver. Enquanto não for resolvido o local fica isolado. (I2) Há um gabinete mesmo que faz auditoria de sistemas de informação da CECV
C.2 Principais benefícios e implicações resultantes da certificação ISO 27001	(I3) Obriga-nos a ter uma certa postura de segurança (I3) Benefícios para os nossos clientes (I3) Garante que a CECV está preocupada com a questão da cibersegurança e proteção de dados pessoais (I3) Melhoria da reputação da instituição (I3) Melhoria nas operações do dia a dia da CECV (I3) Melhoria do aspeto tecnológico (I3) A ISO 27001 não se cinge à parte tecnológica, abrange também os *facilities* de *data center*, (…) os recursos humanos, a entrada e saída de pessoas, a forma como é feita o descarte de dados seja digital ou em suporte papel, como os utilizadores comportam com os dados pessoais dos clientes (a regra de mesa/secretária limpa) (I3) Melhora o nosso desempenho de cibersegurança porque exige-nos uma iniciativa de melhoria continua

D. Cultura Organizacional e Capacitação em Segurança	
D.1 Existência de ações de formação, sensibilização e desenvolvimento em matéria de cibersegurança	(I2) Normalmente não recebemos formações com periodicidade fixa (I2) Tentamos manter-nos sempre informados e acompanhando (I2) Há muita troca de informação e temos pequenas formações com uma empresa parceira (I2) Basicamente todos os anos há formações e ações de sensibilização/capacitação.
D.2 Principais vulnerabilidades, desafios e ameaças à instituição	(I3) Os maiores desafios que enfrentamos é nessa recorrente do *Ransomware*. Mais de 90% dos *Ransomware* entram através do email. É muito importante a parte de sensibilização dos trabalhadores, mas também a parte de proteção dos sistemas de emails (I3) Outra preocupação é a migração sequencial de dados e aplicações para *cloud* (…) As políticas de segurança que nós utilizamos não cobrem esta nova realidade que é a *cloud* (I3) Também a crescente complexidade no geral de toda a tecnologia de suporte ao digital. Obriga o pessoal técnico a estar constantemente atualizado
D.3 Áreas e oportunidades de melhoria	(I2) Primeiramente é o core business da Caixa, é a área que temos maior preocupação, mas também a área do nosso *home banking.* São o motor da sustentabilidade de todo o negócio da CECV (I3) Uma boa capacidade de resiliência é o ponto de chegada que apontamos todos os nossos esforços. Nunca conseguimos chegar a um ponto de perfeição (…) há sempre novas oportunidades de melhoria. (I3) Tendo em conta que a instituição ainda não enfrentou nenhum ataque significativo, pode-se dizer que as estratégias de mitigação são eficazes.

APÊNDICE G: QUESTIONÁRIO DESTINADO AOS COLABORADORES (Q1)

Caro(a) Colaborador(a),

Chamo-me **Ilídio Mendes**, aluno do 2º ano de **Mestrado em Gestão de Instituições Financeiras** no Instituto Superior de Contabilidade e Administração de Lisboa (ISCAL), e estou a realizar um estudo na CECV para a minha dissertação de mestrado. O objetivo do estudo é **avaliar as estratégias de mitigação de riscos cibernéticos na CECV**.

A sua participação é fundamental para o sucesso deste estudo. O questionário é totalmente anônimo e todas as informações fornecidas serão tratadas com a máxima confidencialidade e utilizadas exclusivamente para fins acadêmicos.

Desde já, agradeço a sua colaboração. Com os melhores cumprimentos,

Ilídio Mendes (ilidio.mendes6@gmail.com)

Seção 1: Dados de identificação

1. Género:
   a) Masculino
   b) Feminino
   c) Prefiro não dizer
2. Indique a sua idade: _____
3. Indique o seu nível de escolaridade:
   a) Sem escolaridade
   b) Ensino básico
   c) Ensino secundário
   d) Ensino superior
4. Qual o departamento em que trabalha:
   a) Operacional
   b) Administrativo
   c) Comercial
   d) Informática, Comunicação e Segurança
   e) Marketing

f) Financeiro
g) Outro (especificar) _____

5. Tempo de serviço na CECV: _____

Seção 2: Conhecimento e Formação

6. Na CECV, já recebeu alguma formação/iniciativa (capacitação técnica, ações de sensibilização, entre outros) em matéria de cibersegurança?
   a) Sim
   b) Não
7. Com que frequência participa de ações de formação em cibersegurança?
   a) Anualmente
   b) Semestralmente
   c) Trimestralmente
   d) Nunca
8. Quão satisfeito(a) está com a capacitação em cibersegurança oferecido pela CECV?
   a) Muito satisfeito(a)
   b) Satisfeito(a)
   c) Neutro(a)
   d) Insatisfeito(a)
   e) Muito insatisfeito(a)
9. Está ciente de que a CECV é certificada pela norma ISO 27001 (gestão da segurança da informação) desde 2012?
   a) Sim
   b) Não
10. Quão frequentemente utiliza os procedimentos e políticas de segurança da informação estabelecidos pela ISO 27001 em suas atividades diárias?
    a) Sempre
    b) Frequentemente
    c) Ocasionalmente
    d) Raramente
    e) Nunca

11. Reconhece melhorias trazidas pela ISO 27001 na segurança da informação da CECV e dos clientes?
    a) Sim, significativamente
    b) Sim, moderadamente
    c) Neutro
    d) Não, pouco
    e) Não, em nada

Seção 3: Perceção sobre Riscos Cibernéticos

12. Quão preocupado(a) está com os riscos cibernéticos na CECV?
    a) Muito preocupado(a)
    b) Preocupado(a)
    c) Neutro(a)
    d) Pouco preocupado(a)
    e) Nada preocupado(a)
13. Quais dos seguintes ataques cibernéticos conhece? (Marque todas as que se aplicam)
    a) Engenharia Social (Phishing/Smishing/Vishing)
    b) Malware
    c) Ransomware
    d) Ataques DDOS
    e) Outros (especificar) _____
14. Quais dos seguintes ataques cibernéticos considera as maiores ameaças cibernéticas para a instituição? (Marque todas as que se aplicam)
    a) Engenharia Social (Phishing/Smishing/Vishing)
    b) Malware
    c) Ransomware
    d) Ataques DDoS
    e) Outros (especificar) _____
15. Considera o recurso humano (colaboradores em geral) o ponto mais vulnerável para a entrada de ciberataques na CECV?
    a) Sim
    b) Não
    c) Outro (especificar) _____

Seção 4: Eficácia das Estratégias de Mitigação

16. Como avalia a eficácia das políticas de cibersegurança e mitigação de riscos cibernéticos da instituição?
    a) Muito eficaz
    b) Eficaz
    c) Neutro(a)
    d) Ineficaz
    e) Muito ineficaz
17. A instituição sofreu algum incidente cibernético significativo até à data?
    a) Sim
    b) Não
    c) Não sei
18. Quão eficaz é a resposta da instituição a incidentes cibernéticos?
    a) Muito eficaz
    b) Eficaz
    c) Neutro(a)
    d) Ineficaz
    e) Muito ineficaz
19. Já foi alvo de alguma tentativa de ataque de algum dos seguintes ataques cibernéticos? (Marque todas as que se aplicam)
    a) Engenharia Social (Phishing/Smishing/Vishing)
    b) Malware
    c) Ransomware
    d) Ataques DDOS
    e) Outros (especificar) _____
    f) Nenhuma

Seção 5: Melhoria e Sugestões

20. Quais áreas das estratégias de mitigação de riscos cibernéticos acredita que precisam de melhorias? (Marque todas as que se aplicam)
    a) Políticas e procedimentos
    b) Plano de resposta a incidentes
    c) Formação e consciencialização

d) Tecnologias de segurança
e) Monitorização a incidentes
f) Auditorias e avaliações
g) Outros (especificar) _____

21. Tem alguma sugestão específica para melhorar as estratégias de mitigação de riscos cibernéticos na CECV?

_____

_____

Seção 6: Feedback Geral

22. Por favor, forneça qualquer comentário adicional sobre a cibersegurança na CECV:

_____

_____

OBRIGADO!

APÊNDICE H: QUESTIONÁRIO DESTINADO AOS CLIENTES (Q2)

Prezado(a),

Chamo-me **Ilídio Mendes**, aluno do 2º ano de **Mestrado em Gestão de Instituições Financeiras** no Instituto Superior de Contabilidade e Administração de Lisboa (ISCAL), e estou a realizar um estudo na Caixa Económica de Cabo Verde (CECV) para a minha dissertação de mestrado. O objetivo do estudo é **avaliar as estratégias de mitigação de riscos cibernéticos na CECV**.

A sua participação é fundamental para o sucesso deste estudo. O questionário é totalmente anônimo e todas as informações fornecidas serão tratadas com a máxima confidencialidade e utilizadas exclusivamente para fins acadêmicos.

Agradeço desde já a sua colaboração. Com os melhores cumprimentos,

Ilídio Mendes (ilidio.mendes6@gmail.com)

Seção 1: Dados de Identificação:

1. Tipo de cliente:
   a) Particular
   b) Empresa
2. Se a resposta anterior for “Particular”, indique o seu gênero: (Empresas, por favor ignorem a questão)
   a) Masculino
   b) Feminino
   c) Prefiro não dizer
3. Se a resposta à questão 1 for “Particular”, indique a sua idade: (Empresas, por favor ignorem a questão) _____
4. Se a resposta à questão 1 for “Particular”, indique o seu nível de escolaridade: (Empresas, por favor ignorem a questão)
   e) Sem escolaridade
   f) Ensino básico
   g) Ensino secundário
   h) Ensino superior

5. Há quanto tempo é cliente da CECV? _____

Seção 2: Utilização de Serviços Online

6. Com que frequência utiliza o serviço internet banking da CECV (CaixaNet)?
    a) Diariamente
    b) Semanalmente
    c) Mensalmente
    d) Raramente
    e) Nunca
7. Quais serviços da CaixaNet mais utiliza? (Marque todos os que se aplicam)
    a) Consulta de saldo
    b) Transferências bancárias
    c) Pagamento de contas
    d) Aplicações financeiras
    e) Outros (especificar) _____

Seção 3: Perceção de Segurança e Experiência com incidentes cibernéticos

8. Quão seguro sente-se ao utilizar os serviços de internet banking da CECV?
    a) Muito seguro
    b) Seguro
    c) Neutro
    d) Inseguro
    e) Muito inseguro
9. Qual o nível de confiança que tem para com a CECV?
    a) Muito confiante
    b) Confiante
    c) Neutro
    d) Pouco confiante
    e) Nada confiante
10. Já foi alvo de alguma tentativa de ataque cibernético à sua conta na CECV, por exemplo, acesso não autorizado à sua conta?
    a) Sim
    b) Não
    c) Não sei

11. Se sim, qual foi o ataque? (Considere descrever em poucas palavras o ataque)

_____

_____

12. Se a resposta à questão 10 for “Sim”, quão satisfeito(a) ficou com a resposta da CECV ao incidente?
    a) Muito satisfeito(a)
    b) Satisfeito(a)
    c) Neutro(a)
    d) Insatisfeito(a)
    e) Muito insatisfeito(a)

Seção 4: Conhecimento e Formação

13. Já recebeu alguma comunicação da CECV sobre práticas de segurança na internet (ações de sensibilização entre outros), incluindo na utilização do serviço CaixaNet?
    a) Sim
    b) Não
    c) Não me lembro
14. Sabia que a CECV é certificada pela norma ISO 27001 (gestão da segurança da informação) desde 2012?
    a) Sim
    b) Não
15. Pelo facto da CECV ser uma instituição certificada pela ISO 27001, aumenta a sua confiança na instituição?
    a) Sim, significativamente
    b) Sim, moderadamente
    c) Neutro
    d) Não, pouco
    e) Não, em nada

16. Quais dos seguintes ataques cibernéticos conhece? (Marque todas as que se aplicam)
    a) Engenharia Social (Phishing/Smishing/Vishing)
    b) Malware
    c) Ransomware
    d) Ataques DDOS
    e) Outros (especificar) _____
17. Sente que possui informações suficientes para proteger suas transações online?
    a) Sim
    b) Não
18. Quais fontes utiliza para obter informações sobre a segurança online? (Marque todas as que se aplicam)
    a) Comunicação da CECV
    b) Redes sociais
    c) Notícias (Sites, jornais, televisão, etc.)
    d) Amigos e familiares
    e) Outros (especificar) _____

Seção 5: Feedback e Sugestões

19. Quais medidas de segurança gostaria de ver implementadas no internet banking da CECV?
    a) Autenticação multifator
    b) Alertas em tempo real
    c) Melhoria na interface de usuário
    d) Mais informações sobre práticas de cibersegurança
    e) Outros (especificar) _____

20. Tem alguma sugestão ou comentário sobre como a CECV pode melhorar a segurança dos seus serviços e produtos oferecidos, incluindo CaixaNet?

_____

_____

OBRIGADO!

APÊNDICE I: ANÁLISE DOS RELATÓRIOS E CONTAS 2011, 2012, 2013 E 2023

Documento	Informações Relevantes
Relatório e Contas 2011	Crise financeira mundial Tendência ascendente de inflação e desemprego 2 colaboradores em formação (ISO 27001 Foundation) Ano de consolidação da implementação das recomendações no âmbito da ISO 27001 Investimentos na Tecnologia e Informática: adaptação na *App Banka*; nova imagem do site; versão 3G CaixaNet com nova imagem e novas funcionalidades; Reforço da equipa com mais 2 técnicos; materialização da área de Redes e Sistemas Auditorias informáticas com apoio de consultor externo Criação do Gabinete de Segurança, conclusão da criação da documentação para ISO 27001, inventariação da segurança física Não menciona Gestão de Risco de Informação
Relatório e Contas 2012	Ano da certificação ISO 27001 Acentuação da crise financeira, quebra da atividade financeira da CECV Desaceleração do crescimento da economia Tendência de estabilização de inflação Tendência ascendente de desemprego ISOs 27001 e 9001: 1º Cabo Verde, 2º CPLP, 4º África 6 colaboradores em formação de segurança da infraestrutura tecnológica, método "on-the-job" Tecnologia e Informática: consolidação de vários projetos, auditoria de segurança dos sistemas de informação e implementação das recomendações, migração do Data-Center, upgrade, substituição e reconfiguração de equipamentos de comunicação Implementação de sistema de monitorização de sistemas críticos Não menciona Gestão de Risco de Informação
Relatório e Contas 2013	Sinais lentos de recuperação Contexto ainda desfavorável de crise Auditorias de acompanhamento da ISO 27001 Nº clientes: 259 985 Formação de 11 colaboradores em auditoria interna

	Elaboração de manual de segurança, plano de segurança, plano de emergência e evacuações Implementação de segurança eletrónica dos arquivos Ano de consolidação das recomendações da auditoria de segurança dos sistemas de informação Substituição de todos os PC's de *front office* 1ª auditoria de acompanhamento da ISO 27001 Necessidades de implementação de alguns controlos, maioria associados a procedimentos Não menciona Gestão de Risco de Informação
Relatório e Contas 2023	Diminuição taxa desemprego (Euro 6,4%, EUA 3,8%, CV?) Crescimento PIB Diminuição inflação (3,7%) Líder do mercado em Transformação Digital Aumento da oferta digital: Homebanking CaixaNet, *App* Caixa Mobile, Plataforma Crédito Digital e *App* Caixa Microcrédito Total clientes digitais: 88 647 Transações mais realizadas: consultas de saldo, transferência intrabancárias, pagamento de serviços e carregamento de telemóvel Total clientes: 336 163 (95% particulares) 364 colaboradores ativos (61% femininos, 39% masculinos) Idade média colaboradores: 44 anos Área comercial: 63% dos recursos humanos 69% RH com formação superior Várias sessões de formação no exterior e internamente Soluções digitais levando em conta a cibersegurança Desenvolvimento interno de ferramentas e funcionalidades digitais: DigitalDocs (maior celeridade e desmaterialização de atividades em papel e pouco eficiente); validação de documentos online; SmartBot Modernização tecnológica e fortalecimento da segurança informática: - Manutenções preventivas e corretivas; - Follow-up dos processos de auditoria interna e externa; - Conclusão do projeto de upgrade de redes; - Renovação de licenciamentos como Microsoft, Office, HP, McAfee, RPA, *App*le/Google entre outros; - Implementação da E-fatura, permitindo a faturação de valores que estavam pendentes de liquidação;

	- Implementação no Western Union de canais de número móvel: Whats*App* e Viber; - Aquisição e substituição de servidores pela equipa de administração de sistemas e testes de continuidade de negócio; - Formação dos técnicos de segurança eletrónica e atualização em sistemas de segurança eletrónica; - Projeto de nova Central de Riscos; - Implementação de sistemas de segurança. Framework de Apetite ao Risco (RAF); Inclusão do Risco dos sistemas de informação na Gestão de Riscos.