INSTITUTO
UNIVERSITÁRIO
DE LISBOA

A Realidade da Cibersegurança nas Organizações Portuguesas

Patryck Lino Dumit

Mestrado em Gestão Aplicada

Orientadora:
Prof. Doutora Sofia Lopes Portela, Professora Auxiliar,
ISCTE-IUL

Março, 2023

BUSINESS
SCHOOL

Departamento de Marketing, Operações e Gestão Geral

A Realidade da Cibersegurança nas Organizações Portuguesas

Patryck Lino Dumit

Mestrado em Gestão Aplicada

Orientadora:
Prof. Doutora Sofia Lopes Portela, Professora Auxiliar
ISCTE-IUL

Março, 2023

Agradecimentos

Para a minha família, ficam aqui meus agradecimentos por todo o apoio e compreensão das horas investidas no estudo quando eram necessárias em outra esfera da minha vida.

Aos amigos, meus agradecimentos pelas conversas sobre o estado atual e o futuro da Segurança da Informação.

Por fim, meus agradecimentos à orientadora e ao ISCTE Executive Education por propor este tema e fornecer uma educação de alta qualidade.

Resumo

O ciberespaço português tem evoluído de forma acelerada ao passo do cenário global, no entanto as organizações portuguesas têm sofrido impactos graves de cibersegurança que estão a se tornar mais frequentes devido a alguns influenciadores como o uso de tecnologias emergentes para vantagem competitiva, mas sem o conhecimento necessário para manuseá-las, bem como a falta de manutenção dos sistemas de informação.

A cibersegurança tem como principal objetivo assegurar que as operações de negócio da organização sejam realizadas de forma segura, portanto, a falta dela indica que a mesma está a aceitar riscos tecnológicos elevados e que, possivelmente, podem se concretizar em um ataque ocasionando danos à reputação, à finanças e disrupção nas suas atividades operacionais.

Este estudo traz o tema cibersegurança através de diferentes perspetivas dos setores privado e público, com ênfase no período da pandemia COVID-19, pois as fraquezas se tornaram mais evidentes aos olhos dos clientes e consumidores.

O intuito deste estudo é identificar as principais preocupações das organizações portuguesas de diferentes segmentos e tamanho de estruturas internas, assim como as consequências da falta de segurança cibernética e os investimentos em cibersegurança mais urgentes. Também faz parte do objetivo deste estudo identificar fatores críticos de sucesso transversais nesta matéria para os diversos tipos de organizações portuguesas.

A tese tem como principal objetivo entender o estado atual da cibersegurança em Portugal e como ela tem sido aplicada nas organizações que atuam no país, portanto a metodologia utilizada foi um inquérito aberto ao público português, nomeadamente instituições públicas e empresas privadas.

Palavras-chave: Segurança da Informação; Risco; Cibersegurança, Mudança organizacional.

JEL Classification:
O33 - Technological Change: Choices and Consequences • Diffusion Processes;
M15 - IT Management

Abstract

The Portuguese cyberspace has evolved at an accelerated pace following the global scenario, however Portuguese organizations have suffered serious cybersecurity impacts and are more frequent due to internal and external forces such as the use of emerging technologies for competitive advantage, but without the necessary knowledge and the lack of maintenance of the information systems.

Cybersecurity has as its main objective to ensure that the entity's operational activities are carried out safely, therefore, the lack of it indicates that the entity is accepting high technological risks and that, possibly, may materialize in an attack causing damage to the reputation of the entity and disruption in its operational activities.

This study brings the cybersecurity theme through different perspectives of the private and public sectors, with an emphasis on the period of the COVID-19 pandemic as weaknesses have become more evident in the eyes of customers and consumers.

The purpose of this study is to identify the main concerns of Portuguese organizations from different segments and internal structures, as well as the main impacts that might occur due to lack of information security and the most urgent investments in cybersecurity. It is also part of the objective of this study to identify critical success factors in this subject for organizations regardless of their size and the segment in which they operate.

The main objective of the thesis is to understand the current state of Cybersecurity in Portugal and how it has been applied in organizations that operate in the country, so the methodology used was an open survey to the Portuguese audience, namely public institutions and private companies.

Keywords: Information Security; Risk; Cybersecurity, Organizational Change.

JEL Classification:
O33 - Technological Change: Choices and Consequences • Diffusion Processes;
M15 - IT Management

Índice

Índice de Figuras

Glossário

API - Permite que um aplicativo solicite dados ou serviços de outro aplicativo.

CID - Abreviatura para “Confidencialidade, Integridade e Disponibilidade”. São os três pilares básicos da Segurança da Informação.

CNCS - Centro Nacional de Cibersegurança.

Due Care - É um termo legal utilizado para descrever o cuidado que “uma pessoa razoável” tomaria sob determinadas circunstâncias, utiliza-se para descrever a obrigação legal de um indivíduo ou organização e a falta de “due care” é normalmente considerada como negligencia.

Due Dilligence - É uma medida preventiva tomada para evitar danos a outras pessoas ou sua propriedade, é uma prática que deve ser adotada pelos profissionais de segurança da informação como princípio básico em suas carreiras. Exemplos de “due diligence” incluem verificar os antecedentes de funcionários, crédito de parceiros de negócio, avaliação da segurança dos sistemas.

IoT - Capacidade de conectar qualquer dispositivo à internet (ou a outro dispositivo) com um simples botão liga/desliga, com o intuito de transmitir e receber dados que melhoram a performance e usabilidade do dispositivo.

IIoT - Abreviatura do termo em inglês “Industrial Internet of Things”, referente aos equipamentos industriais IoT.

NIST - National Institute of Standards and Technology.

Phishing - É um tipo de crime cibernético que consiste na utilização de práticas fraudulentas e o uso de engenharia social para roubar ou obter informações pessoais de suas vítimas, como senhas, dados bancários, números de cartão de crédito, entre outros.

PSI - Política de Segurança da Informação.

SI - Segurança da Informação.

Risco - Probabilidade de um evento acontecer multiplicado pelo impacto deste evento caso se concretize. Os riscos de segurança cibernética estão relacionados à perda de confidencialidade, integridade ou disponibilidade de informações.

1. Introdução

A segurança da informação tem preocupado cada vez mais as organizações portuguesas devido ao seu dinamismo mais rápido do que a evolução tecnológica que as organizações podem adotar. Quando esta matéria é bem implementada com tecnologias que respondem as dificuldades da entidade na educação e formação adequadas para colaboradores e prestadores de serviço, aliadas a políticas robustas que fornecem diretrizes para a organização, o risco de cibersegurança ao qual a entidade está suscetível é consideravelmente menor quando comparado à uma outra que não segue pelo mesmo caminho.

Um influenciador de extrema importância é o ambiente externo que aos dias de hoje traz à vista de todos os problemas de segurança da informação e as consequências perante a opinião pública e esferas legais. Apesar de não ser possível controlá-lo, o ambiente externo pode ser compreendido e, a partir dele, aprender quais são as técnicas defensivas e ofensivas ideais para assegurar que os serviços e produtos fornecidos pela organização estão seguros. Com isso, os riscos de segurança e corporativos podem ser evitados ou mitigados contribuindo para uma resiliência operacional mais robusta.

É com base nisso que este estudo visa compreender a realidade do quesito segurança da informação nas organizações portuguesas, com foco nas suas principais preocupações em meio a pandemia, seus motivos para não ter a segurança da informação corretamente implementada e as possíveis consequências nas quais a organização está exposta, métodos comumente utilizados para implementar esta matéria e as obrigações legais que acompanham a segurança da informação. Ao agregar o contexto atual e tendências a isto, este estudo também traz sugestões de fatores críticos de sucesso transversais a qualquer organização, independentemente da sua área de atividade.

Os resultados apresentados nesta tese têm como base o inquérito realizado com as empresas públicas e privadas, de diversos tamanhos, setores de atividade e são uma amostra de como é a estratégia da SI, as dificuldades técnicas e organizacionais, assim como as preocupações das organizações portuguesas e das estrangeiras com presença no país.

No capítulo dois, Revisão da Literatura, são abordados os conceitos básicos de cibersegurança e segurança da informação, que muitas vezes são utilizados de maneira intercambiável, no entanto possuem suas diferenças e que são a base para toda a tese. Neste capítulo também são abordados os motivos e as consequências da falta de segurança da informação numa organização e como evitar a falta desta matéria. Outros conceitos presentes neste capítulo são as obrigações legais associadas à SI, as principais preocupações, a

progressão da maturidade de SI numa organização e, por fim, os fatores críticos para o sucesso.

No capítulo três, é apresentado o contexto atual da segurança da informação no espaço cibernético, com foco no cenário nacional através das perspetivas das entidades governamentais e institutos de pesquisa, no cenário internacional através das perspetivas das agências europeias e pesquisas realizadas por empresas da área e nas tendências para o futuro da SI, utilizando como base as novas tecnologias estudadas que estão a ser estudadas, preocupações e previsões de empresas conceituadas na área.

Nos capítulos quatro e cinco, respetivamente, são descritas em maiores detalhes a metodologia utilizada e apresentados os resultados do inquérito, que passam por mostrar as principais preocupações e consequências da falta de SI, à luz do que foi abordado no capítulo dois.

Nos capítulos seis são abordados as propostas de ações às organizações portuguesas para o desenvolvimento da maturidade de SI face ao contexto atual nacional, internacional, tendências para um futuro próximo e o inquérito respondido por organizações presentes no país. No capítulo sete são apresentadas as conclusões do estudo, onde é delineado um perfil de SI das organizações portuguesas face às necessidades do ambiente externo e a sugestões de respostas para os desafios à frente.

2. Revisão de Literatura

Esta secção descreve a revisão da literatura relevante para a cibersegurança, desde a sua definição até os fatores que a circulam como as legislações, regulamentos, pontos fracos e fortes mais comuns nos diferentes setores empresariais.

2.1. Definição de Cibersegurança e Segurança da Informação

A informação é um ativo crucial nos tempos atuais e sua proteção tornou-se algo essencial para o sucesso das organizações num ambiente competitivo. A cibersegurança, de acordo com o Centro Nacional de Cibersegurança (2021), pode ser definida como "conjunto de medidas e ações necessárias para prevenir, monitorizar, detetar, analisar e corrigir redes e sistemas de informação face às ameaças a que estão expostos, tentando manter um estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, pode, por outro lado, ser definido como o sentimento de segurança percecionado pelas pessoas quando usam a Internet e as tecnologias digitais". A Segurança da Informação cobre as matérias de cibersegurança, bem como outras como segurança de redes de computadores, segurança física e é definida pelo *National Institute of Standards and Technology – NIST* (2022) como a proteção de informações e sistemas contra acesso, uso, divulgação, interrupção, modificação ou destruição não autorizados, para fornecer confidencialidade, integridade e disponibilidade.

A segurança da Informação, ao seu nível mais básico, pode ser resumida em três pilares comumente chamadas de *CID*, acrónimo que representa as três bases Confidencialidade, Integridade e Disponibilidade. Uma empresa que deseja implementar um projeto, seja ele uma solução técnica ou apenas uma estrutura de políticas, normas e procedimentos, deve seguir estas bases como uma boa prática para atingir seus objetivos de segurança cibernética. De acordo com Antunes et al. (2021) são muitos os dados das operações de uma organização e sua confidencialidade é uma grande preocupação, exigindo que um conjunto de procedimentos e regras dentro da organização seja aplicado para definir quem tem acesso aos dados e informações. Integridade e Disponibilidade focam na confiabilidade e precisão dos dados acedidos por pessoas autorizadas. Assim, os padrões e frameworks de segurança da informação são fundamentados na implementação de políticas e controlos, para gerir a segurança e os riscos ao nível organizacional.

2.2. Motivos para falta de segurança da informação nas organizações

A segurança da informação no ambiente corporativo possui uma enorme visibilidade para o Comité Executivo atualmente, portanto se tornou vital para as organizações portuguesas a identificação dos riscos e respetivas ações de mitigação. A segurança da informação deve ser uns dos principais fatores para o sucesso desta matéria em qualquer organização (Burkett, 2021). Devido a diversas outras preocupações corporativas, as empresas não a tornaram uma competência essencial dentre seus colaboradores, ou seja, as pessoas não estão preparadas para situações de ataques cibernéticos ou incidentes que causam indisponibilidade de ativos.

Hart et al. (2017) defende que o suporte do comité executivo sinaliza a importância da segurança da informação para o restante da organização e pode capacitar os funcionários a mudarem a forma como abordam a segurança da informação. Da mesma forma, as atitudes de segurança da informação dos utilizadores provavelmente serão influenciadas pelas normas que caracterizam seu ambiente corporativo, como as expetativas e comportamentos de seus colegas. De facto, o papel da liderança e o suporte do comité executivo, bem como as normas do local de trabalho, estão consagrados em modelos populares de segurança da informação, como, por exemplo, o modelo de negócios ISACA (Citation 2009) para segurança da informação.

Alinhar o programa de segurança com o direcionamento da empresa requer um entendimento sólido da área de tecnologia, como as soluções utilizadas estão posicionadas em toda a empresa, como apoiam o negócio e sua importância comercial, além de entender como especificamente a área da segurança da informação fornece proteção aos ativos e contribui para os objetivos da estratégia corporativa. Desta forma, nasce uma nova abordagem para a governança de segurança que ajuda a ver como a segurança é vista e subsidiada dentro da empresa. O esforço para aumentar o foco em uma abordagem alinhada aos negócios elevará a segurança de uma ação puramente de mitigação para um facilitador de negócios tático para a empresa (Istikoma et al., 2015).

O estudo realizado por CyberEdge Group (2022), o qual teve a participação de 1200 decisores em segurança da informação de 17 países, totalizando numa participação de 19 setores de atividade, concluiu que o maior motivo para a falta de segurança é a falta de profissionais capacitados, seguido por falta de consciencialização da segurança informática entre os colaboradores (Figura 1).

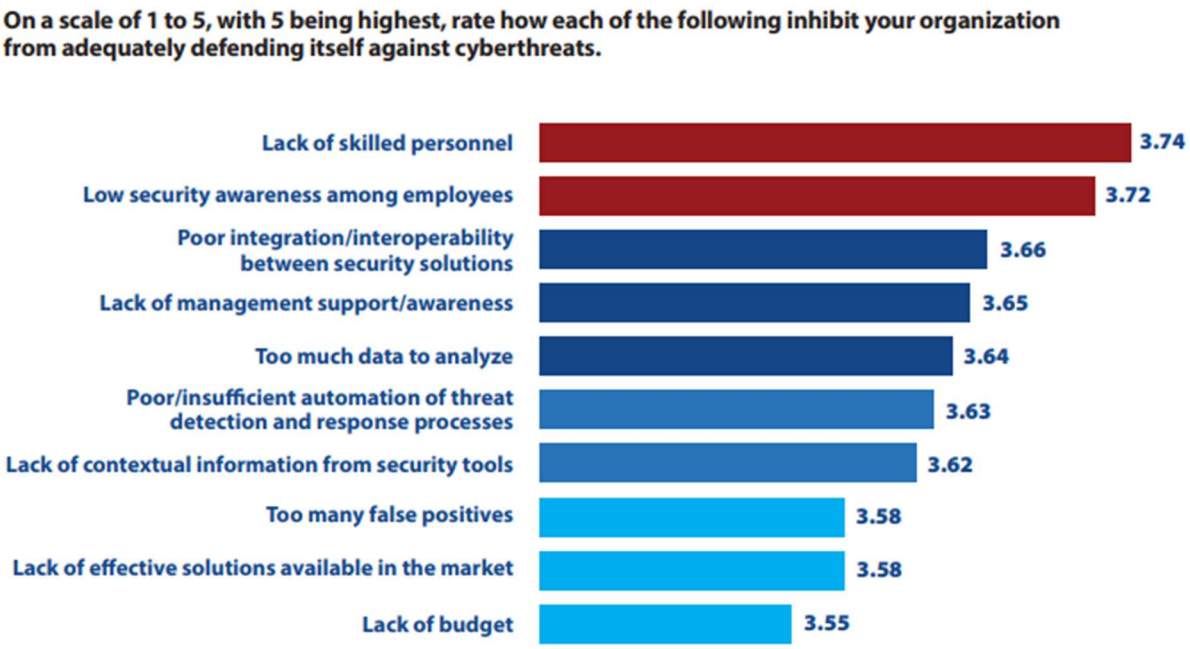

Figura 1: Os 10 maiores motivos para falta de segurança da informação. Fonte: Cyberthreat Defense Report 2021

2.3. Consequências da falta de segurança da informação nas organizações

De acordo com a SANS (2012) ao considerar a implementação de uma tecnologia, uma organização pode pensar que é direito do empregador implementar sistemas e coletar quaisquer dados que escolher com base na preocupação legítima de perder a propriedade intelectual. Esta suposição é incorreta e perigosa. Devem existir diretrizes que sejam seguidas para identificar quando a organização não esteja protegendo os dados pessoais dos funcionários. Não há posição legal para uma organização agir sem cumprir com a lei de privacidade, o que pode deixar a empresa exposta à litígios.

Uma organização que não possui a atenção em matérias de segurança da informação está mais suscetível a incidentes de cibersegurança. O Ministério da Economia (2018) define um incidente de cibersegurança como “qualquer ação não autorizada ou ilegal que envolva computadores (sistemas ou aplicações) ou redes, representando quebras nas medidas de Cibersegurança” e ainda complementa que “as medidas de resposta envolvem o bloqueio do ataque e a reposição do normal funcionamento, bem como a identificação das causas do incidente de forma a prevenir futuros ataques, fraudes e extorsões”, resultando em impactos descritos no estudo como “poderá ficar em causa a reputação das empresas, o dispêndio de recursos financeiros e o registo de perdas financeiras”.

Um incidente de cibersegurança pode ter diversas origens, como ameaças internas ou externas, uma falha operacional, ou até mesmo um evento climático que resulta na indisponibilidade de sistemas. De acordo com a CyberEdge Group (2022), exemplos de

cibercrimes são os crimes como fraude através da manipulação de registos, quebra de controlos de segurança, acesso não autorizado ou modificação do sistema, roubo de propriedade intelectual, pirataria informática, manipulação de mercados (e.g. ações), roubo de identidade, propagação de spam e de malware, negação de serviço ou criação e distribuição de conteúdo ilegal.

2.4. Como evitar a falta de segurança da informação nas organizações

Num mundo globalizado e extremamente dependente da tecnologia da informação, a falta de atenção ao que acontece no ciberespaço e em como a organização pode ser afetada aumenta o risco cibernético, resultando em possíveis danos financeiros, reputacionais e também em impactos nas operações conduzidas pela empresa. De acordo com Bruma (2020), a escolha de não investir em segurança da informação pode impactar, por exemplo, em decisões de fusão e aquisições aquando do momento da realização do *due care* e *due dilligence,* ou também em definições de estratégia ao nível executivo para os próximos anos, ou ainda nas decisões de colaborar ou não com um fornecedor. Existem maneiras de uma organização não cometer o mesmo erro ano após ano, ao estar atenta ao ciberespaço e realizar uma análise do próprio perfil e compará-lo com o perfil desejado. Esta abordagem é utilizada pelo *framework* "*NIST CyberSecurity Framework*", que foi criado pela entidade governamental norte-americana NIST, utiliza as terminologias "*Current Profile*" e "*Target Profile"* para identificar o esforço eficiente a ser considerado para implementar uma postura de segurança da informação eficaz (NIST, 2016; p.4). O NIST revela no seu *website* um caso de sucesso onde a Intel, empresa multinacional do setor de tecnologia, usou a estrutura de segurança cibernética num projeto piloto para comunicar o risco de segurança cibernética à liderança sénior, melhorar os processos de gestão de risco e aprimorar seus processos para definir prioridades de segurança e os orçamentos associados a essas atividades de melhoria (NIST, 2022).

Uma outra maneira é realizar auditorias internas ou externas para verificar a eficácia dos controlos implementados nos níveis organizacionais, táticos e operacionais comparados aos controlos descritos num *framework* ou padrão internacional, geralmente a ISO/IEC 27001:2013. De acordo com Antunes et al. (2021), a norma ISO/IEC 27001:2013 é um padrão internacional que define uma lista de controlos que devem ser considerados na implementação de um Sistema de Gestão de Segurança da Informação (SGSI). Como organizações de todos os tipos e portes coletam, processam, armazenam e transmitem dados e informações, eletronicamente, fisicamente e verbalmente, o padrão foi concebido para ser utilizado como referência e proposta de melhores práticas, na implementação de um SGSI

num amplo conjunto de cenários e setores de atividade. A prática da auditoria recorrente, geralmente anual, serve como um motivador para a implementação de melhorias que coletivamente melhoram a postura da organização em relação a segurança da informação e diminui os riscos cibernéticos, tanto da probabilidade quanto do impacto, que podem afetar a empresa.

2.5. Progressão da maturidade de segurança da informação

Antunes et al. (2021) defende que a segurança da informação se torna relevante numa organização quando surgem desafios desta matéria e devido a isto é definido o uso adequado de tecnologias, as estruturas organizacionais e um conjunto de documentos normativos para responder às exigências de controlos, nomeadamente políticas, processos, procedimentos. Ao estabelecer, implementar e monitorizar esses controlos, um nível mais alto de consciencialização sobre a necessidade e a importância da segurança, os objetivos de negócios da organização são alcançados.

2.5.1. Pessoas

Recentemente os relatos de ataques cibernéticos tornaram-se frequentes e utilizam-se das pessoas como um ponto de entrada, pois é considerado o elo mais fraco na segurança da informação, nomeadamente os colaboradores da empresa, os fornecedores e prestadores de serviço e a segurança cibernética da empresa é tão forte quanto o elo mais fraco da corrente. Portanto, é necessário ter um ponto de partida para implementar com sucesso controlos que mitigam ataques e técnicas mais simples que podem ser facilmente reconhecidas por pessoas, independente da área em que atuam. Adicionalmente, em 2020 os colaboradores transitaram para um modelo de teletrabalho, em alguns casos sem nenhuma instrução, ou equipamento corporativo ou ambos, portanto é irrealista a expetativa de que as pessoas tenham o conhecimento necessário para se prevenirem de ataques cibernéticos. De acordo com um estudo realizado pela fabricante russa Kaspersky Labs (2018), 52% das empresas relataram que os colaboradores constituem a fraqueza mais significativa em termos de cibersegurança e a Verizon (2021) afirma que 85% das violações de dados envolvem o elemento humano.

Para responder a isto deve ser criado um Plano de Consciencialização em Segurança da Informação, que deve existir formalmente na empresa com o objetivo de educar e avaliar regularmente os utilizadores, gerar métricas e ações de melhorias ajustadas à realidade da empresa. A Agência da União Europeia para Cibersegurança, ENISA (2021), afirma em seu relatório anual que o Plano de Consciencialização é uma das principais recomendações para

mitigar as probabilidades de *ransomware* na empresa, através de treinamento apropriado e utilização de simulação de cenários para identificar ataques de engenharia social e campanhas de *phishing*. É através da prática e da repetição do que foi aprendido que os colaboradores podem reter conhecimento e adquirir competências de cibersegurança ao alto nível para saber responder às ameaças cibernéticas (Beats e Van der Linden, 2003).

Ao olhar com foco maior para o *ransomware*, é possível perceber que as empresas industriais sofreram mais devido ao elevado nível de automatização dos sistemas e pouca instrução aos operadores em termos de cibersegurança. A *Capgemini Research Institute* (2021) afirma, em sua pesquisa realizada com 950 empresas, que 80% das organizações concordam que a cibersegurança é um componente crucial (Figura 2) e 73% das organizações no mundo afirmam que sofreram um ataque cibernético nos últimos 12 meses em suas fábricas inteligentes (Figura 3), ou seja, fábricas que utilizam a tecnologia *Industrial Internet of Things* (IIoT).

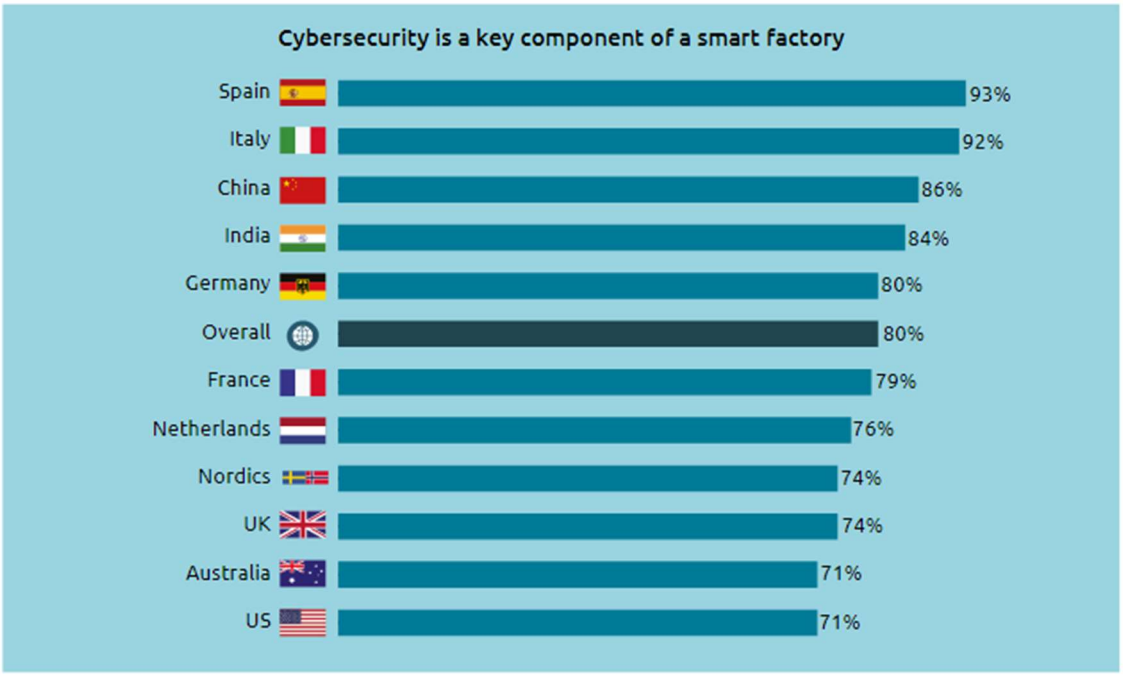

Figura 2: Ranking de países que utilizam a cibersegurança como componente principal em fábricas inteligentes (Fonte: Cybersecurity in Smart Factories, p. 19)

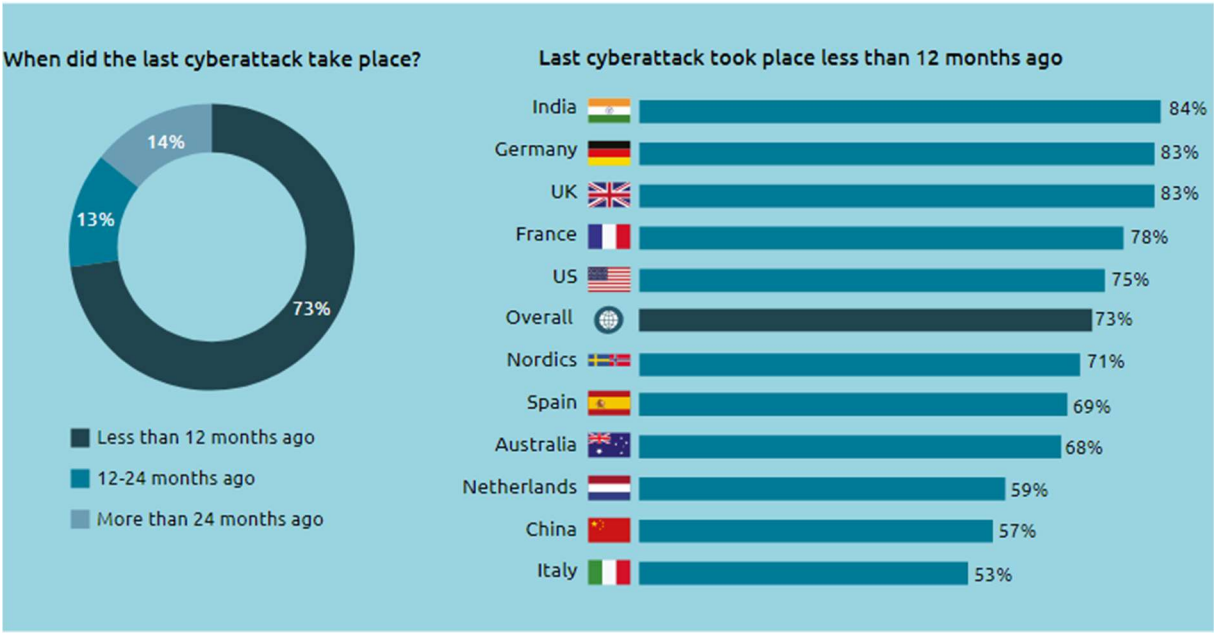

Figura 3: Estatísticas de ciberataques em fábricas inteligentes (Fonte: Cybersecurity in Smart Factories, p. 13)

De acordo com a pesquisa realizada pela Capgemini Research Institute (2021) existem várias etapas para a mitigação dos problemas e a principal, defende a pesquisa, é que a gestão organizacional desenvolva uma consciência da gravidade da atual falta de preparação para ataques cibernéticos, para que priorize a segurança cibernética das fábricas inteligentes. Para enfatizar a importância disso, 94% dos líderes realizam treinamento interno regular e programas de consciencialização sobre segurança cibernética para o comité executivo e complementa que dada sua infraestrutura de treinamento mais forte, os líderes estão em uma posição muito melhor em termos de preparação dos que não possuem tal infraestrutura. Dentre os líderes, 81% dizem que sua equipa de segurança cibernética (funcionários/fornecedores no local) possui o conhecimento e as habilidades relevantes para realizar correções de cibersegurança urgentes de forma independente e eficaz sem suporte externo, em comparação com 48% dos que não possuem tal conhecimento.

Além da realidade das fábricas inteligentes e seus problemas com *ransomwares*, o relatório da ENISA (2021) defende que as práticas que compõem um programa de consciencialização auxiliam na prevenção e mitigação do impacto causado pelas campanhas de *phishing* e de desinformação. O relatório aponta que estas campanhas possuem as seguintes características:

- O *phishing* está no centro dos ataques de desinformação e explora fortemente as crenças das pessoas;
- As ameaças centradas no ser humano são difíceis de analisar em termos pragmáticos, incluindo a capacidade de as descrever, decompor, classificar e

reproduzir para alimentar análises quantitativas, simulações gráficas ou numéricas ou codificação em algoritmos;

- Os ataques de desinformação se beneficiam da dificuldade de quantificar tudo o que está relacionado com humanos. Quando a ameaça envolve ou depende do comportamento das pessoas (por exemplo, erros, viés cognitivo, falta de habilidades), medições e coleta de dados são processos complexos que geralmente resultam em dados de baixa qualidade;
- O problema da desinformação não é a capacidade de distinguir informações verdadeiras ou falsas; em vez disso, é uma crise social amplificada pelo contexto político;
- A desinformação que está se movendo das esferas políticas/sociais para o mundo corporativo está crescendo em escopo e impacto graças às plataformas de rede social e tecnologias de criação de conteúdo.

2.5.2. Processos

Os documentos normativos atuam na lacuna entre as pessoas e as tecnologias e geralmente são definidos em três níveis: políticas, normas e procedimentos. Este conjunto precisa fazer parte do programa de formação e consciencialização para fornecer as instruções que os utilizadores devem seguir, portanto este conjunto, também chamado de processos, deve ser revisto anualmente para serem eficazes (SANS, 2012; p.16), atualizados em relação ao ambiente externo e com o Comité Executivo. Uma empresa que almeja elevar o nível de maturidade organizacional em matéria segurança da informação deve ter uma paragem obrigatória para formalizar, por escrito, as diversas diretrizes definidas pelo Comité Executivo e diretores em um conjunto de documentos normativos, que servirão para orientar os funcionários e prestadores de serviço nas diferentes situações as quais a empresa e as pessoas estão sujeitas.

Antunes et al. (2021) defende que as melhores práticas dentro de uma organização são vitais e representam a linha de frente dentro da segurança da informação. A definição de políticas deve ser o primeiro desafio para proteger os dados organizacionais e definir os procedimentos a serem seguidos. O objetivo é definir um nível de proteção para garantir que os dados e as redes organizacionais estejam seguros e protegidos. Estes autores ainda complementam que os *frameworks* e standards que são referência no setor, como a ISO/IEC 27001, têm como definição básica a criação e implementação de políticas e processos para atingir o nível básico de maturidade.

Uma política de segurança da informação (PSI) é essencial para uma implementação bem-sucedida desta matéria e é definida pela SANS como a base de qualquer programa de

segurança da informação e é de propriedade da liderança sénior dentro de uma organização. Políticas eficazes fornecem declarações que incluem o que é aceitável, não aceitável e as consequências da violação da política, como perda de emprego ou ação legal. Esses são itens que os utilizadores devem seguir e estas não são orientações ou recomendações (SANS, 2012; p.18). A SANS (2021) também defende que as políticas devem ser publicadas para que todos na organização possam facilmente ter acesso às mesmas. Os utilizadores finais devem ser notificados imediatamente quando as políticas forem alteradas e sempre que ocorrer uma violação, para uma correção ágil. Eles também precisam ser revistos, no mínimo, anualmente para garantir que estejam atualizados e abordem as ameaças atuais e a direção dos programas de segurança. Uma revisão semestral é a melhor prática, pois força as organizações a revalidar as políticas atuais contra as ameaças mais recentes. A SANS (2021) ainda conclui que a PSI auxilia na reputação da empresa pois o objetivo da política de segurança digital de uma organização é definir os procedimentos, diretrizes e práticas para configurar e gerir a segurança em seu ambiente. Ao aplicar a política, as corporações podem minimizar seus riscos e mostrar a devida diligência para seus clientes e acionistas.

Outro exemplo é a definição do período de retenção de dados, a partilha de informação corporativa para parceiros de negócio e clientes, entre outras definições, através da classificação da informação, que deve ser formalizada numa Política de Classificação da Informação. A classificação da informação pode ser definida como um elemento crítico para reforçar a proteção de dados e que deve ser utilizada para responder, por exemplo, questões como o nível de confidencialidade, a quem pertencem os dados e qual o tipo de proteção deve ser implementado, portanto, a política de classificação da informação ou proteção de dados deve exigir que todos os documentos sejam classificados. Deve incluir também o sistema de classificação a ser utilizado para que os utilizadores saibam o que, como e o porquê para classificar os documentos (SANS, 2012; p.19). O interessante de ressaltar neste ponto é que não há uma estrutura de classificação “correta”, tornando fácil para uma organização customizar os níveis de confidencialidade de acordo com a sua realidade e um exemplo disto é a NATO, entidade composta por diversos países, possui os seguintes níveis de classificação da informação, do menos ao mais restrito respetivamente: NATO Unclassified (Figura 4), NATO Restricted, NATO Confidential, NATO Secret e Cosmic Top Secret (Figura 5). Portanto, é possível perceber que cada organização, pública ou privada, deve criar ela própria sua estrutura e educar as pessoas para que entendam quando utilizar cada nível de classificação. Outro aspeto importante que deve estar numa política de classificação da informação é o processo de revisão da classificação de um documento (Figura 6), para que reflita com exatidão sua importância para a empresa.

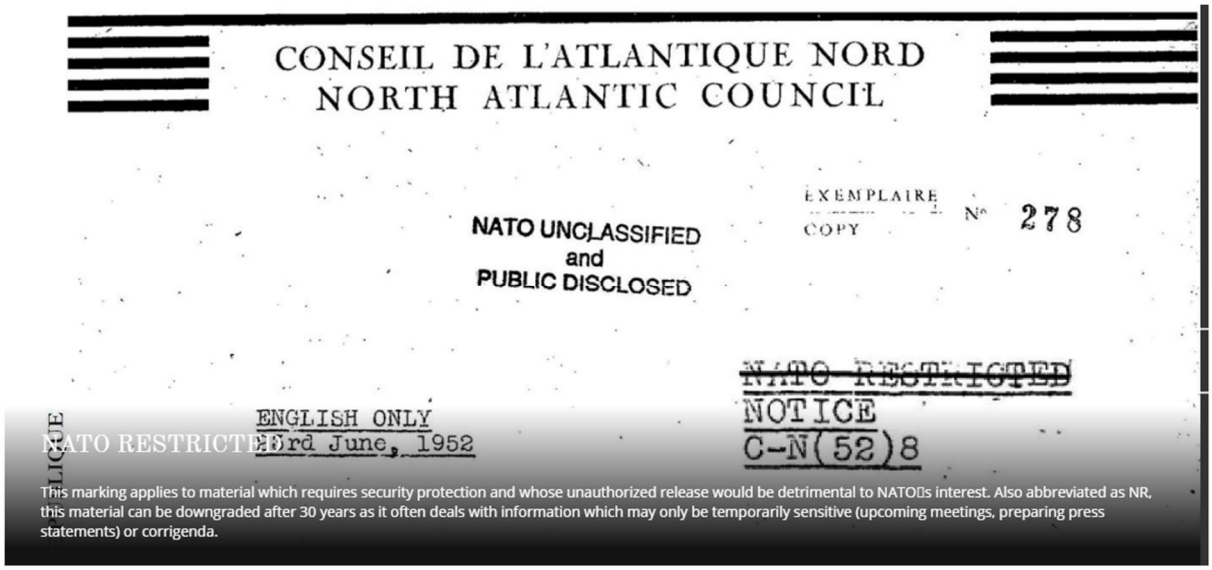

Figura 4: artigo “For Your Eyes Only: What is security classification?” (Fonte: NATO)

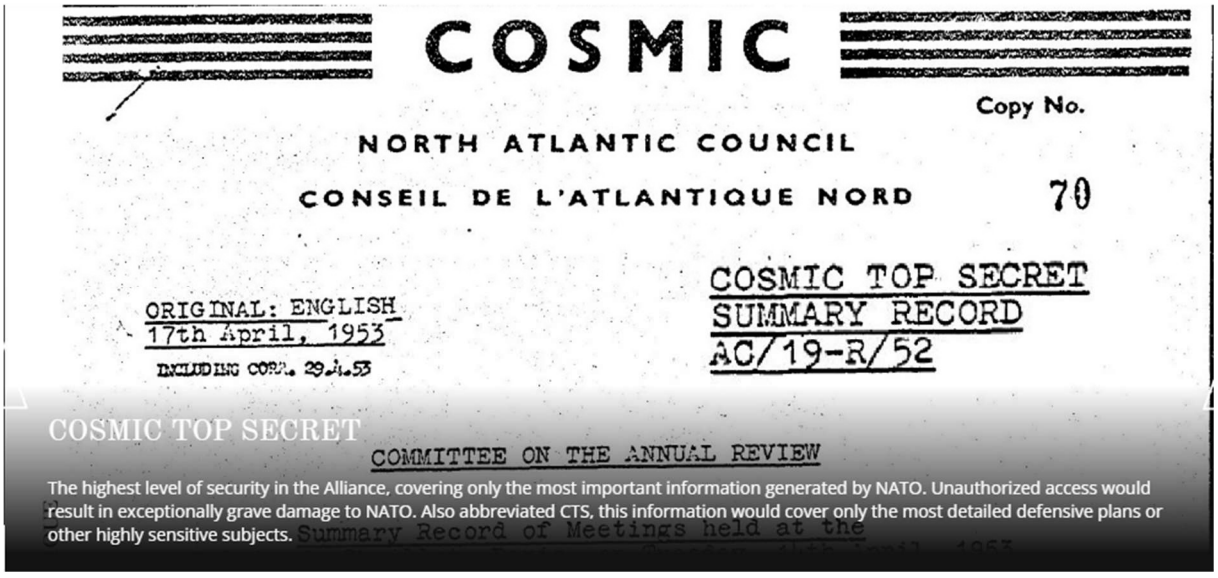

Figura 5: artigo “For Your Eyes Only: What is security classification?” (Fonte: NATO)

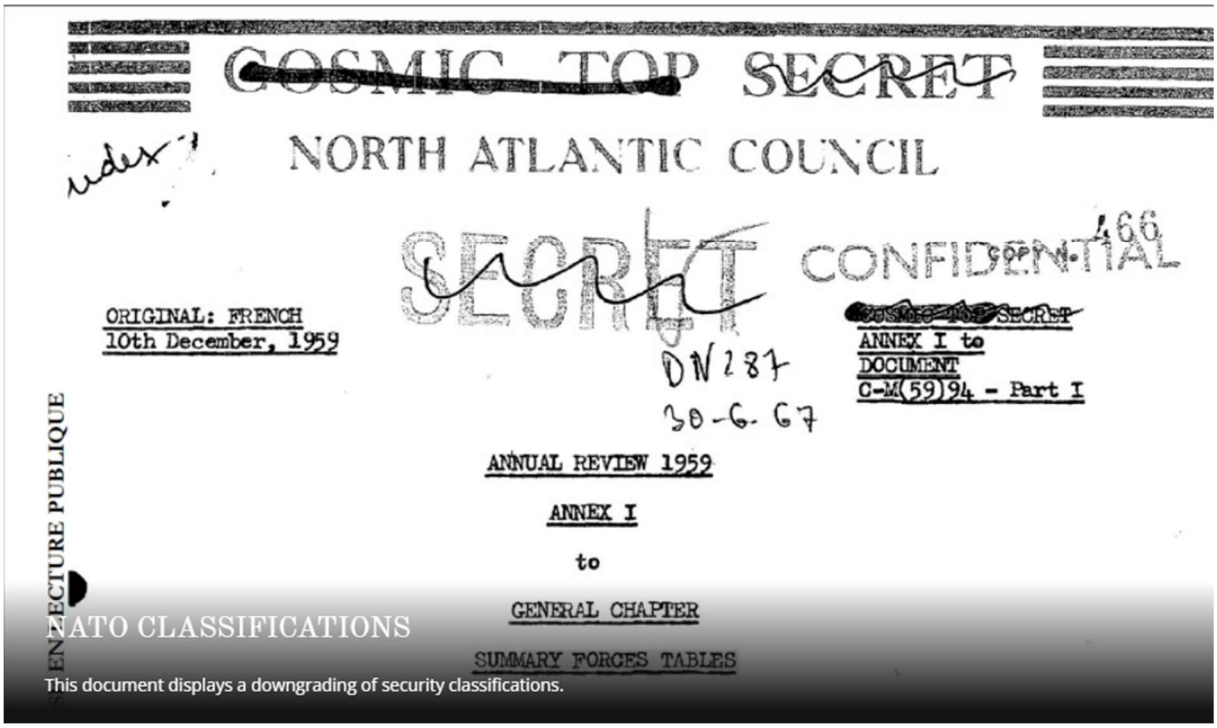

Figura 6: artigo “For Your Eyes Only: What is security classification?” (Fonte: NATO)

2.5.3. Tecnologias

As soluções tecnológicas no campo da segurança da informação têm evoluído em um ritmo acelerado nos últimos anos e prova disso é o conceito de solução em nuvem, ou em inglês *cloud computing*, onde há pouco mais de cinco anos não se conversava sobre isto e atualmente é quase uma obrigatoriedade devido aos benefícios que o conceito apresenta e é com base nisto que o relatório do CyberEdge Group (2022) identificou os países com maiores percentagens de uso da computação em nuvem para serviços e aplicações de segurança da informação (Figura 7).

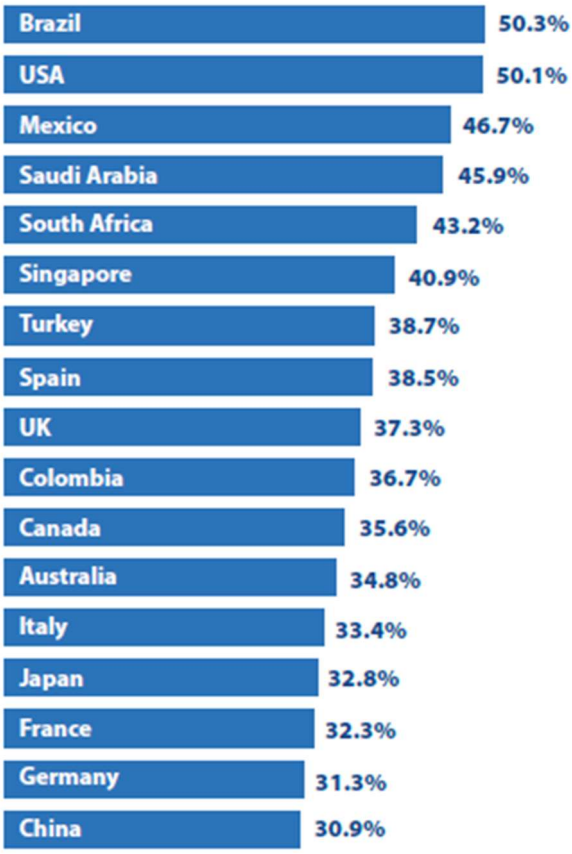

Figura 7: Percentagem de serviços e aplicações de segurança fornecidas através da computação em nuvem, por país (CyberEdge Group, 2022; p.48)

Aliado a este conceito, outros também se tornaram necessários e, no âmbito da segurança da informação, o mais importante é o conceito de "confiança zero", originalmente chamado de "*zero-trust*", no qual ultrapassa o modelo antigo de olhar para os equipamentos no perímetro da rede corporativa como fronteira entre o confiável e não confiável, para introduzir o modelo de que todo equipamento e toda identidade não são confiáveis, esteja ele na "nuvem" ou no datacenter mantido pela empresa. Em outras palavras, o portátil e o utilizador de rede são considerados não confiáveis e, desta forma, são implementados controlos para garantir que equipamentos e identidades estão seguros antes e durante a conexão com a rede corporativa, trazendo mais segurança para a empresa, permitindo que pessoas se conectem a partir de qualquer lugar de forma segura e viabilizando, por exemplo, cenários de acesso remoto e teletrabalho. Collier e Sarkis (2021) defendem que confiança zero não é uma tecnologia ou configuração de rede específica, mas sim um novo paradigma para pensar sobre confiança e segurança. Com base na suposição de que nenhum utilizador ou dispositivo em uma determinada rede pode ser confiado implicitamente, independentemente do tráfego de rede se originar da rede da empresa ou externamente, a confiança zero estabelece um conjunto de princípios e políticas orientadores para serem feitos à cada solicitação de acesso, permitindo decisões de confiança baseadas em autenticação e

autorização tanto da identidade quanto do dispositivo, com base na coleta e monitorização contínua e detalhada dos dados. A confiança zero é, acima de tudo, uma postura defensiva.

Desbonnet (2022) ressalta três razões principais pelas quais a adoção da abordagem de confiança zero faz sentido para os negócios de uma empresa:

- A implementação de uma abordagem de confiança zero preparará melhor uma organização para mudanças em tecnologia, regulamentação, geopolítica, cultura e até novas parcerias. Ele não apenas permite que as empresas estejam à frente das mudanças antes que elas aconteçam, mas também permite que elas acelerem as iniciativas de transformação digital com menor risco ao mesmo tempo;
- A confiança zero reforça o suporte aos negócios. Ao criar políticas de confiança eficazes, como aquelas em que as pessoas mudam de função, a abordagem reduz os riscos associados ao facto de pessoas erradas terem acesso às informações que não deveriam. Ao implementar uma melhor identificação de ativos, as empresas obterão melhor visibilidade geral de redes confiáveis, que se aplicam tanto a novos empreendimentos e aquisições quanto às pessoas;
- Por fim, o resultado para TI e segurança será uma arquitetura simplificada e económica, com uma visão clara dos riscos técnicos e melhor prevenção dos riscos comuns. Também abre as portas para a segurança sem senha, o que facilitará a proteção do local de trabalho no futuro.

Desbonnet (2022) conclui que implementar o modelo confiança zero não é apenas um projeto com data de término, mas uma tarefa de monitorização contínua da infraestrutura, por exemplo, configurando sensores que podem detetar atividades incomuns ao monitorizar quem, o quê, onde e como os dados são utilizados. Isso significa implementar autenticação moderna de utilizador que usa, por exemplo, biometria ou *tokens* no lugar de senhas, uma solução de monitorização de dispositivos, bem como da sua localização e rastreamento de uso de aplicativos corporativos. Esses recursos são impulsionados pelo software de deteção que permite que o sistema de monitorização gerencie novos conteúdos e conjuntos de casos de uso como base para deteção de anomalias. Aliado a uma visão geral do risco das identidades, é possível consolidar a visibilidade da postura de segurança e obter uma melhor compreensão das áreas prioritárias que requerem investimentos para implementar soluções técnicas.

2.6. Principais preocupações das organizações em matérias de cibersegurança

A pesquisa de mercado realizada pelo CyberEdge Group (2022) concluiu que entre as principais preocupações de segurança da informação, a coleta de informações de identificação pessoal (Personally Identifiable Information – PII) é a maior de todas, seguida de perto por roubo de credenciais (Figura 8).

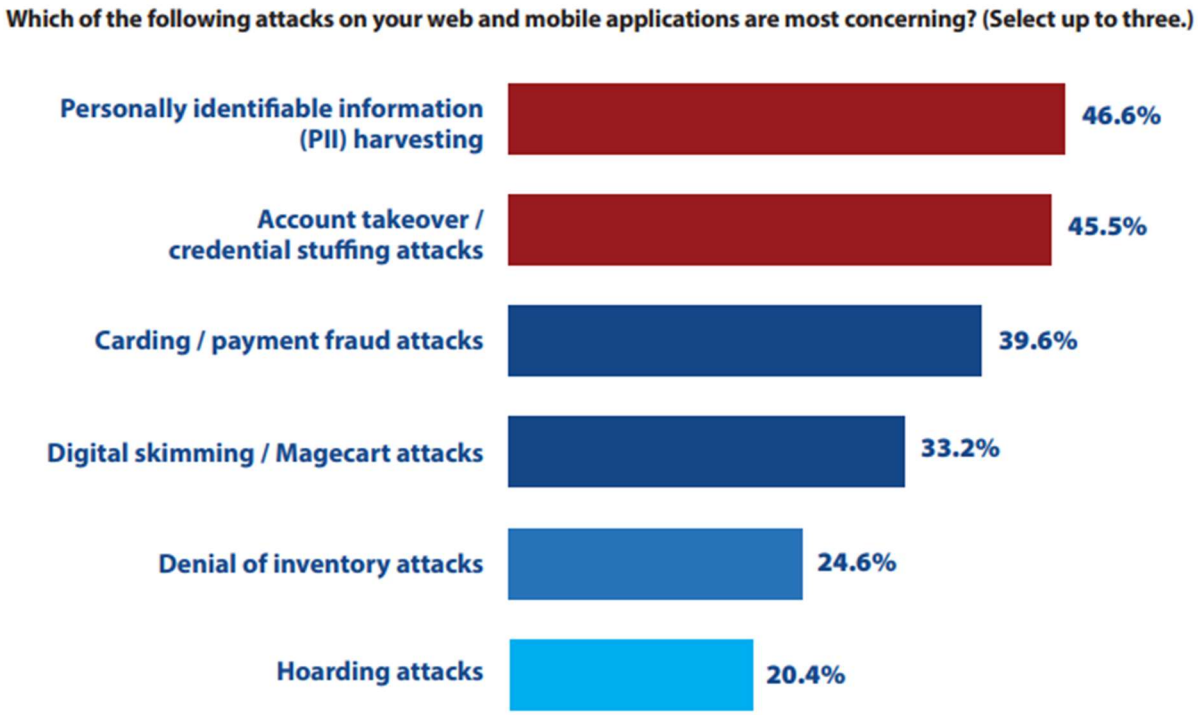

Figura 8: Maiores preocupações em segurança da informação (Cyberdge Group, 2022; p.19)

No entanto, de acordo com a pesquisa do CNCS (2022), no âmbito nacional as organizações portuguesas tiveram o seu foco em 2021 direcionado para outras preocupações, entre elas a principal é o *phishing* seguido por *ransomware*. A mesma pesquisa já projetava para 2022 um aumento de casos de *ransomware*, ocupando a primeira posição do ranking de ciberameaças mais relevantes (Figura 9). A pesquisa realizada pelo CNCS (2022) demonstra que os ciberataques que se utilizam de engenharia social com intuito de roubar credenciais, informações e dados pessoais e sequestrar dados empresariais prevaleceram nos últimos anos. Além disso, o teletrabalho trouxe facilidades e conforto para o colaborador, mas trouxe dificuldades na gestão da segurança pois não há mais o "perímetro" antes facilmente identificado pelas fronteiras da infraestrutura da empresa que separavam o ambiente interno do mundo externo.

2020			2021			Ordenação		Perspetivando 2022		
RK	Tipo	%	RK	Tipo	%	Tend./ pp	Lugar RK	Tipo	%	Tend./RK 2021/2022
1º	Phishing/Smishing	89	1º	Phishing/Smishing	89	=	=	Ransomware	93	+
2º	Ransomware	65	2º	Ransomware	89	+ 24	=	Phishing/Smishing	87	-
3º	Engenharia social	58	3º	Engenharia social	65	+ 7	=	Engenharia social	74	=
4º	Exploração de vulnerabilidade	52	4º	Exploração de vulnerabilidade	59	+ 7	=	Exploração de vulnerabilidade	70	=
5º	SPAM	47	5º	SPAM	46	- 1	=	Software malicioso	52	+
6º	Comprometimento de conta	47	6º	Comprometimento de conta	41	- 6	=	Comprometimento de conta	50	=
7º	Software malicioso	41	7º	Software malicioso	48	+ 7	=	Scanning aos sistemas	46	+
8º	Tentativa de *login*	35	8º	Tentativa de *login*	35	=	=	DoS/DDoS	33	+
9º	Scanning aos sistemas	30	9º	Scanning aos sistemas	35	+ 5	=	SPAM	30	-
10º	DoS/DDoS	27	10º	DoS/DDoS	30	+ 3	=	Tentativa de *login*	28	-

Figura 9: Ciberameaças mais relevantes 2020, 2021 e projeção para 2022. (Fonte: CNCS)

2.7. Obrigações legais das organizações em termos de segurança da informação

A União Europeia está liderando o esforço para regular a defesa contra ameaças cibernéticas nos níveis normativo/legal e estratégico. Por meio dessa estratégia, a Comissão Europeia procurou criar legislação para criminalizar tais crimes, aumentar a capacidade de segurança cibernética e promover a troca de informações entre países (Carvalho et al., 2020; p.4).

De acordo com Carvalho et al. (2020), outro marco importante no campo dos regulamentos e legislações foi a publicação da Diretiva (UE) 2016/1148, também conhecida como NIS Directive, que fornece instruções para garantir um alto nível comum de segurança de rede e informação em toda a União Europeia. Esta Diretiva define que cada Estado-Membro deve adotar uma Estratégia Nacional e criar um Grupo de Cooperação para reforçar a colaboração e troca de informações para obter uma resposta rápida a incidentes, definindo ainda a designação de autoridades nacionais competentes e as obrigações de comunicação dos prestadores de serviços digitais e operadores de serviços essenciais (infraestruturas do mercado financeiro, energia, transportes, saúde, abastecimento e distribuição de água potável e infraestruturas digitais). Desde sua publicação, esta Diretiva sofreu duas atualizações, em 2018 e 2022. A primeira atualização pode ser resumida nos principais pontos:

- Um Pacote de Cibersegurança que estabelece medidas concretas para responder às ameaças reais;
- Preparar uma resposta eficaz em caso de ciberataques que afetem vários Estados-Membros;
- Uma proposta para reforçar a ENISA como uma nova Agência Europeia de Cibersegurança, a fim de garantir que a Agência presta apoio aos Estados-Membros, instituições da UE e empresas em áreas-chave;
- Criação de instrumentos de implementação da Diretiva (UE) 2016/1148, ou seja, orientações sobre como a Diretiva deve funcionar na prática;
- Um compromisso com uma Certificação Europeia para tornar os dispositivos conectados mais seguros (estrutura comum de certificação de segurança cibernética).

A última atualização, UE 2022/2555, que foi aprovada pelo Parlamento Europeu (2022), redefine as classificações serviços críticos e serviços essenciais, bem como aumenta o escopo de organizações que estão sujeitas à Diretiva. Além disso, a Diretiva também define valores financeiros mínimos para coimas e prazos para notificações de incidentes de cibersegurança. Esta recente atualização, denominada Diretiva NIS 2, ainda precisa ser transposta para legislações nacionais de cada Estado-Membro no máximo até 17 de Outubro de 2024.

Ainda a nível europeu, uma medida criada para responder à crescente procura de proteção de dados foi a introdução do Regulamento Geral de Proteção de Dados (RGPD) (UE) 2016/679, como revogação da Diretiva de Proteção de Dados 95/46/EC. Este regulamento foi aprovado em 15 de abril de 2016 e, após um período transitório de dois anos, entrou em vigor em 25 de maio de 2018 e é definido como um regulamento europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia e Espaço Económico Europeu (EEE). Destina-se a dar aos cidadãos e residentes formas de controlar seus dados pessoais e pretende-se também unificar a União Europeia como marco regulatório sobre privacidade e proteção de dados pessoais, bem como uma forma de regular a exportação de dados pessoais fora da UE e do EEE (Carvalho et al., 2020; p.5).

O RGPD possui requisitos e cláusulas que descrevem a maneira como os dados pessoais devem ser tratados desde a recolha até o seu descarte e é aplicável às organizações que operam no EEA (EU, 2016), que em 2019 foi transposta em legislação portuguesa (Lei 58/2019). Em resumo, alguns dos principais requisitos do RGPD são (Carvalho et al., 2020; p.5):

- Os processos de negócio que tratam de dados pessoais devem ser desenhados de raiz e por defeito com medidas que respeitem os princípios de proteção de dados;
- Os dados devem ser armazenados usando pseudonimização ou anonimização completa, com as mais altas configurações de privacidade por padrão, para que os dados não possam ser disponibilizados sem consentimento explícito e não possam ser usados para identificar alguém sem informações adicionais armazenados separadamente;
- O processamento de quaisquer dados fora do contexto legal especificado no regulamento não é permitido, exceto quando o controlador de dados tiver recebido consentimento explícito e opt-in do proprietário dos dados. Os dados são propriedade do proprietário, que tem o direito de revogar esta permissão a qualquer momento;
- O responsável pelo tratamento deve indicar claramente qualquer recolha de dados, indicar qual o enquadramento legal que permite tal recolha de dados, a finalidade do tratamento dos dados, durante quanto tempo os dados serão armazenados e se esses dados serão partilhados com terceiros fora da União;
- Os utilizadores europeus têm o direito de exigir uma cópia dos dados coletados em formato comum e o direito de exigir que esses dados sejam excluídos em determinadas circunstâncias;
- As autoridades públicas e as empresas que privilegiam o tratamento regular ou sistemático de dados pessoais são obrigadas a ter um Encarregado de Proteção de Dados (DPO), que é responsável por assegurar que o tratamento está em conformidade com o RGPD;
- As empresas são obrigadas a relatar qualquer violação de dados em até 72 h quando houver qualquer efeito adverso na privacidade do utilizador.

Naturalmente, Portugal transpôs estas e outras Diretivas em legislação nacional para refletir os requisitos em obrigações legais. O estudo “Cibersegurança em Portugal” do Ministério da Economia descreve que em 15 de Setembro de 2009, foi aprovada a Lei do Cibercrime, “procurando dar segurança aos cidadãos e instrumentos às entidades que enfrentam a Cibercriminalidade” (Ministério da Economia, 2018; p.43).

Em 2012, o Governo de Portugal considerou essencial a consolidação das iniciativas em uma Estratégia Nacional de Segurança da Informação, ocasião na qual resultou na criação do Centro Nacional de Cibersegurança (CNCS). No ano seguinte foi revisto o Conceito Estratégico de Defesa Nacional tendo em conta a necessidade de proteger o funcionamento da economia e da sociedade da informação do Ciberterrorismo e da Cibercriminalidade

(Ministério da Economia, 2018; p.44). Desde então, ocorreram atualizações anuais onde em 2015 a estratégia nacional foi descrita como "(i) promover a consciencialização, uso livre, seguro e eficiente do ciberespaço, (ii) proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos; (iii) fortalecer e garantir a segurança do ciberespaço, de infraestruturas críticas e de serviços nacionais vitais e (iv) afirmar o ciberespaço como um lugar para o crescimento económico e a inovação". A estratégia também definiu cinco objetivos:

- Estruturar a segurança do ciberespaço;
- Combater o Cibercrime, Proteger o ciberespaço e as infraestruturas nacionais;
- Promover a educação, a consciencialização, a prevenção;
- Fomentar a cooperação;
- Incentivar a investigação e desenvolvimento.

As empresas também precisam estar atentas a obrigações legais específicas para o setor em que atuam, como a área da Saúde, Finanças, Seguros, Telecomunicações e diversas outras. Chapple et al. (2018) defende que as principais legislações e regulamentos para cada setor de atuação são as Legislações de privacidade dos Estados Unidos, o RGPD, a Lei de Privacidade Canadiana e em destaque o CCPA (*California Consumer Privacy Act of 2018)*.

As legislações que tratam de privacidade nos Estados Unidos são do âmbito federal, onde se destacam:

- 4ª Emenda da Constituição;
- *The Privacy Act of 1974;*
- *Electronic Communication Privacy Act of 1986;*
- *Communication Assistance for Law Enforcement (CALEA) of 1994;*
- *Economic Espionage Act of 1996;*
- *Children's Online Privacy Protection Act of 1998*;
- *Health Insurance Portability and Accountability Act (HIPPA) of 1996*.

Este último, foi aprovado pelo congresso americano, que estabeleceu regulamentos de privacidade e segurança que exigem medidas rigorosas para hospitais, médicos, companhias de seguros e outras organizações que processam ou armazenam informações médicas privadas sobre indivíduos. A HIPAA também define claramente os direitos dos indivíduos sujeitos a registos médicos e exige que as organizações que mantêm esses registos divulguem esses direitos por escrito (Chapple et al., 2018; p.142). Em 2013 foi aprovada pelo Congresso um complemento ao HIPAA, chamado HITECH - *Health Information Technology for Economic and Clinical Health Act of 2009*, com o objetivo de dar mais rigor na relação entre uma organização no âmbito do HIPAA e seus parceiros de negócio que lida com informações

de saúde privadas (PHI – *Protected Health Information),* além de criar também requisitos para que empresas notifiquem o vazamento de tais dados (Chapple et al., 2018; p.143).

Para as organizações que atuam na área de Finanças, uma das obrigações legais de destaque é a GLBA – Graham Leach-Bliley Act, que possui a descrição oficial "empresas que oferecem produtos ou serviços financeiros aos consumidores, como empréstimos, consultoria financeira ou de investimento, ou seguros – para explicar suas práticas de partilha de informações aos seus clientes e proteger dados confidenciais" e possui o objetivo de "exigir que as empresas abrangidas desenvolvam, implementem e mantenham um programa de segurança da informação com mecanismos administrativos, técnicos e físicos projetados para proteger as informações do cliente" (Federal Trade Comission, 2022).

Por fim, a União Europeia e os Estados Unidos tinham até 2020 um acordo para troca de informações sensíveis e dados pessoais no âmbito da privacidade e segurança, chamado de *Privacy Shield*. Era necessário que as empresas no escopo do Privacy Shield estivessem em conformidade com os requisitos, o que os garantia um certificado para atestar a conformidade e o direito de partilhar tais informações além da fronteira continental. No entanto, em Julho de 2020, um caso na corte de justiça europeia informalmente chamado de *Schrems II* (Facebook Ireland Ltd vs. Maximillian Schrems) invalidou o acordo conhecido por *Privacy Shield*, deixando empresas desamparadas legalmente (Federal Trade Comission, 2022). Desde então as organizações que precisam partilhar informações além da fronteira continental baseiam-se em modelos de acordo desenvolvidos pela própria empresa ou, em alguns casos, no framework publicado pela *Asia-Pacific Economic Cooperation* (APEC).

2.8. Fatores críticos de sucesso

De acordo com o CNCS (2022), "Relatório Cibersegurança em Portugal - Economia", para que seja reconhecido a evolução da segurança da informação é preciso conhecer as métricas que se devem ter em conta. Tal como em todas as matérias económicas, os recursos disponíveis para aplicar em Cibersegurança são escassos, principalmente em momentos adversos como em períodos de depressão económica e pandemia. É essencial para as organizações disporem de métricas que lhes permitam definir estratégias de Cibersegurança. Para tal, é necessário quantificar os custos e os benefícios das soluções de segurança, associando sempre que possível os custos aos respetivos benefícios, procurando definir o nível de segurança. O CNCS (2022) complementa que o nível de segurança pode ser definido como a forma como os custos suportados permitem reduzir os riscos que as instituições enfrentam e que podem ser medidos considerando indicadores determinísticos (os quais consideram, por exemplo, se existem antivírus instalados) ou estocásticos (os quais refletem

o comportamento dos atacantes, por exemplo o número de situações de bloqueio de intrusões).

No entanto, medir este nível é uma tarefa complexa e o estudo conclui que medir o nível de segurança de uma instituição varia consoante o tipo de organização. Em todo o caso, a análise deverá ter em conta os mesmos fatores em qualquer dos casos. Para tal, é necessário definir indicadores que possam ajudar a definir esse nível. Um dos fatores comuns a todos os casos é a análise de riscos que é definida por Gordon et al. (2003). como o processo de avaliar os riscos, tomar medidas para reduzir o risco a um nível aceitável e manter esse nível de risco. Segundo os referidos autores, a gestão do risco desenvolve-se em 3 fases. As três fases descritas por estes autores representam as etapas de analisar o risco, reduzir o risco ao nível aceitável e, por fim, manter o risco no nível aceitável através da monitorização contínua e, caso o nível aumente, todo o processo deve ser refeito até chegar a um limite aceitável novamente. Gordon et al. (2003) descreve as três fases em detalhes (Figura 10):

- Numa primeira fase, as organizações deverão identificar as ameaças e vulnerabilidades dos seus sistemas de informação;
- Numa segunda fase, as organizações deverão identificar a informação vulnerável que deverá ser alvo de medidas de segurança, procurando reduzir o risco para níveis que sejam considerados aceitáveis, através de ações como investir em proteção contra o risco de ataque e adquirir seguros contra ciberataques para reduzir o risco de perdas financeiras em caso de ataque;
- Atingido o nível de risco aceitável, também chamado de risco residual, é necessário manter esse nível, pelo que as organizações deverão proceder à monitorização contínua do estado dos seus sistemas de informação, bem como investir em sistemas de deteção de ataques e criar planos de contingência para fazer face aos ataques. Naturalmente, o risco residual poderá variar consoante o setor de atividade, a idade ou a dimensão da empresa.

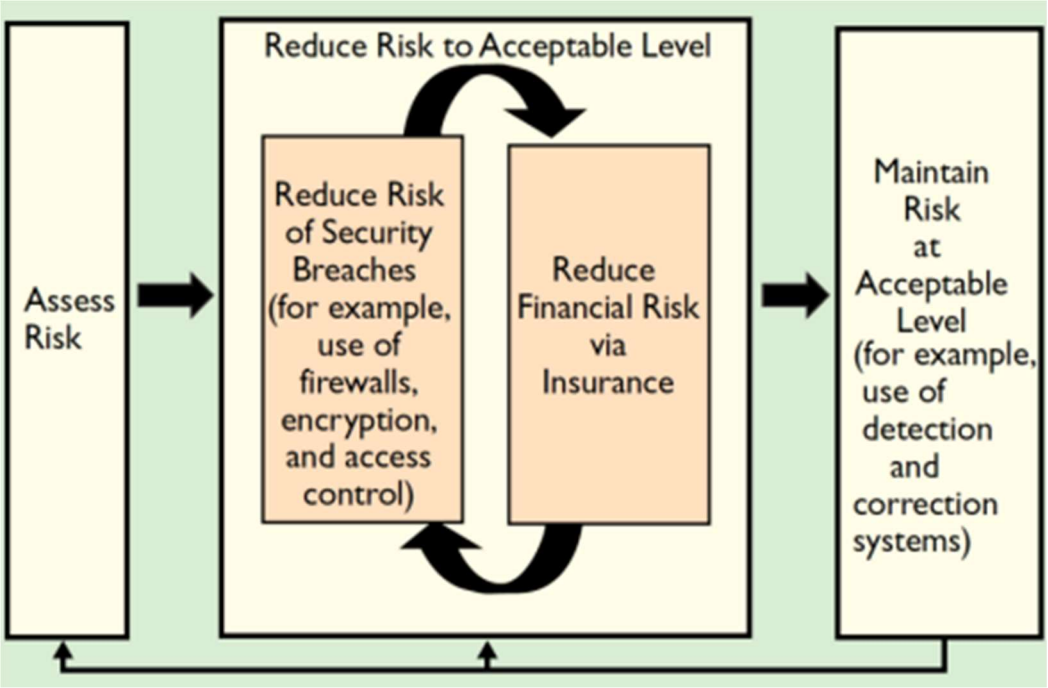

Figura 10: Framework “Gestão de Risco” (Fonte: Gordon et al.)

3. Contexto Atual

No contexto pré-pandémico, o World Economic Forum (2019) identificou uma crescente preocupação de indivíduos, empresas e governos com ciber riscos para o ano de 2019 e à época, 82% dos entrevistados responderam estarem preocupados com roubo financeiro ou de dados e 80% com disrupção nas operações. A pesquisa global revelou ainda que fraude e roubo massivo de dados ocupou a quarta posição, seguido por outros ciberataques, num ranking dos dez maiores riscos num horizonte de dez anos, portanto consolidando os ciber riscos tão importantes como riscos ambientais. No relatório da edição de 2022, o tipo de ataque que teve maior aumento foi o de *ransomware* e está diretamente relacionado ao contexto pandémico e ao despreparo das pessoas quanto ao assunto cibersegurança (World Economic Forum, 2022).

No período da pandemia, especificamente no ano de 2020, o CNCS (2022) realizou um estudo denominado "Cibersegurança em Portugal – 2021" e concluiu que houve um aumento acentuado de cibercrime e incidentes de cibersegurança a partir de março, onde os principais ataques envolviam engenharia social, sequestro de dados, intrusão e burla, resultando numa perceção de aumento de risco de ciberameaças de interesse nacional, onde os principais atores, já nesta época, eram grupos organizados patrocinados financeiramente e tecnologicamente por nações. Outro relatório, realizado pela Capgemini Research Institute (2021*)*, corrobora o aumento de ataques, a nível internacional, através da engenharia social como o *spear-phishing*, ataque de *phishing* direcionado a um alvo específico, que aumentou 667% desde fim de Fevereiro de 2020 a Abril do mesmo ano. A Figura 11 mostra o aumento de incidentes de cibersegurança em Itália, o país com menor percentagem de profissionais diplomados em TIC no ano de 2019.

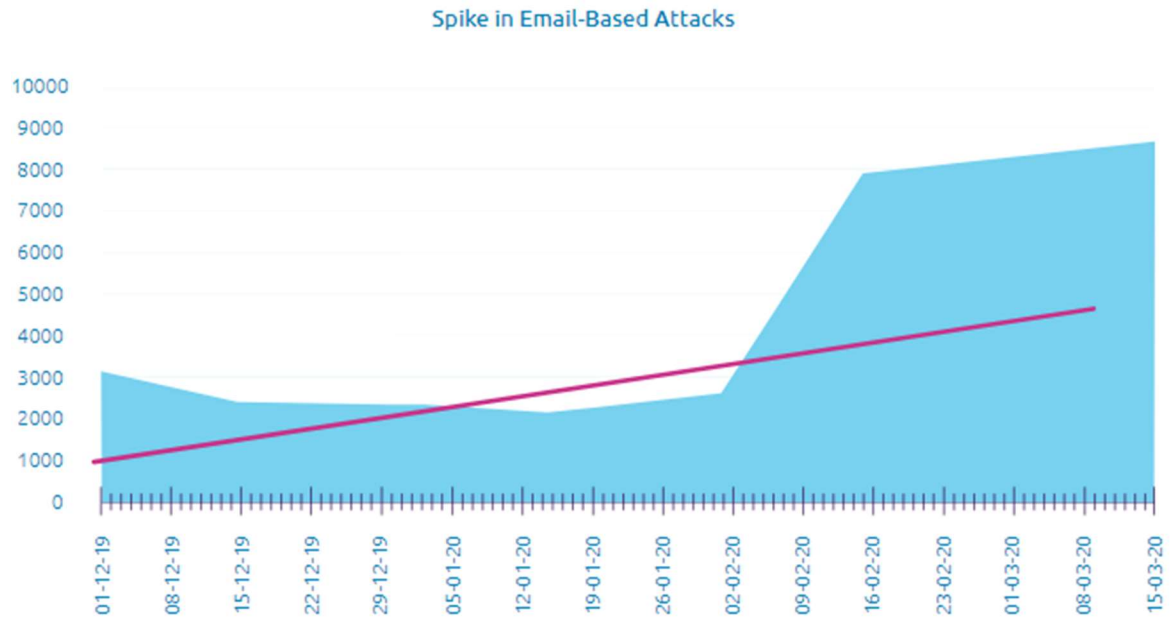

Figura 11: Aumento de ciber ataques por emails (Fonte: ”Boosting Cybersecurity Immunity”, *Capgemini Research Institute*, Abril 2020)

Outro desafio relevante dos últimos anos para a área de cibersegurança são os diplomados em TIC em Portugal (Figura 12), defende o CNCS (2022), pois o país possui a terceira pior percentagem (2,3%) da Europa de diplomados na área, ficando à frente apenas da Bélgica (2,1%) e da Itália (1,3%). Esta percentagem do país português está abaixo da média europeia (3,9%), conforme indica o estudo, que é liderado pela Estónia (8,0%) e Irlanda (7,8%) e não por acaso, recentemente a Estónia esteve a investir em incentivos para atrair imigrantes, principalmente das áreas de tecnologia, com bons ordenados e com promessas de qualidade de vida. Já a Irlanda está a atrair já há alguns anos as *big techs* como Amazon, Facebook, Google, que em troca fornecem visibilidade do país irlandês aos imigrantes.

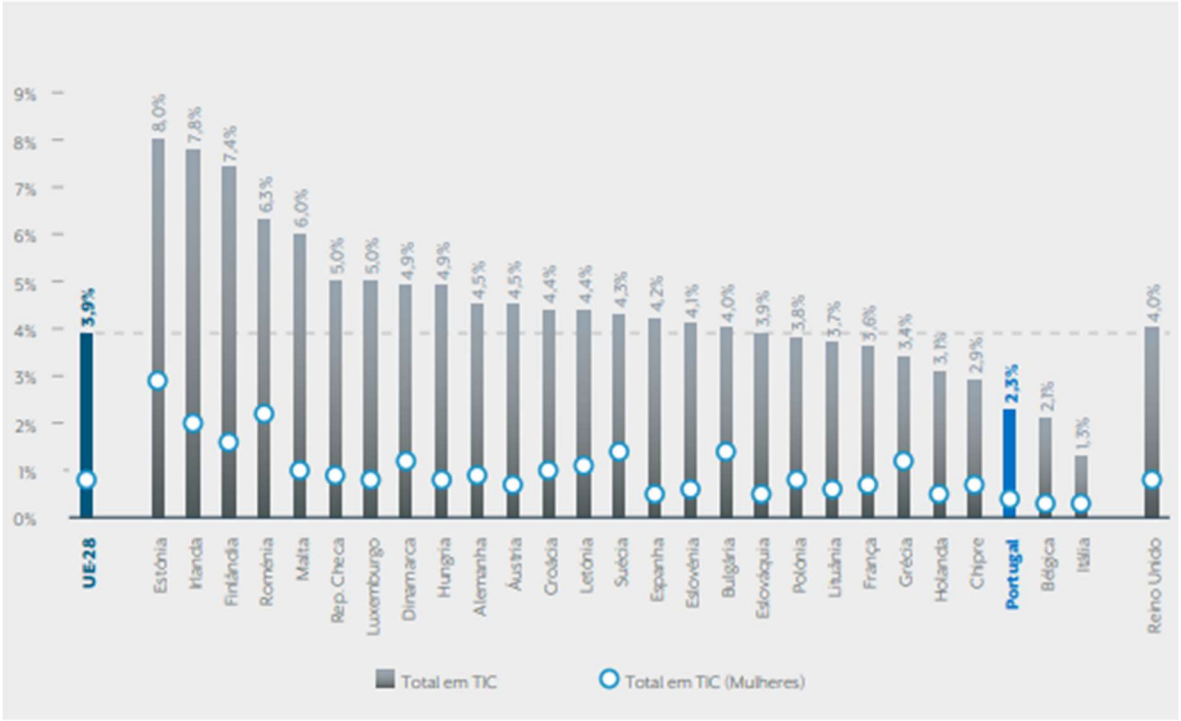

Figura 12: Percentagem de diplomados em TIC, por país (Fonte: Relatório "Cibersegurança em Portugal – Economia 2022", Centro Nacional de Cibersegurança)

3.1. Cenário nacional

As empresas portuguesas estão a enfrentar um ambiente perigoso e cheio de incertezas, onde o quesito resiliência se tornou cada mais necessária devido aos ataques cibernéticos como os que afetaram a Vodafone Portugal e a Germano de Sousa, ambos na mesma semana em Fevereiro de 2022, bem como ao Grupo Impresa em Janeiro de 2022 conforme noticiado nos principais jornais nacionais e é nesse sentido que o relatório publicado pelo CNCS (2022), na altura da pandemia, mostra a tendência de crescimento no volume de crimes cibernéticos manteve-se e outro fator, ainda mais preocupante, é a previsão destes volumes não regressarem ao mesmo patamar pré-pandemia. O mesmo relatório também conclui que o ciberespaço português está muito exposto devido às características do país onde ataques à cadeia de abastecimento, que muitas vezes envolve atores internacionais, afetam o país, a economia e o bem-estar da população.

O CNCS (2022) salienta ainda que a fragilidade do fator humano permanece como o principal vetor de ataque, principalmente para os que estão relacionados com a pandemia, sendo este o foco da atenção de ataques de engenharia social que apelam aos sentimentos como medo e curiosidade, ou para o senso de urgência. Outros ataques como o *ransonware*, também conhecido como sequestro de dados, e a exploração de vulnerabilidades da infraestrutura também são vetores altamente visados, gerando grandes impactos principalmente em empresas industriais e de infraestrutura crítica, como energias e água.

Ataques que têm explorado com sucesso o fator humano através de campanhas de *phishing*, avança este relatório, são realizados por cibercriminosos organizados que visam ganhos financeiros através da fraude online ou o sequestro de dados de empresas de relevância nacional e esta tendência tem acompanhado os crescentes níveis internacionais de ataques homólogos (CNCS, 2022).

3.2. Cenário internacional

No espectro global, seguem-se as mesmas tendências nacionais de ataques que visam as pessoas como principal fragilidade empresarial. O World Economic Forum (2022), que foi respondido por 12,000 líderes ao redor do mundo, conclui que 95% dos incidentes de cibersegurança puderam ser rastreados a um erro humano e em 2020 houve um aumento de 435% em *ransomware* face ao ano anterior (Figura 13). Estes números globais impressionam ainda mais pois o mesmo estudo também conclui que existe uma falta de 3 milhões de profissionais, portanto há um esforço considerável das empresas em formar colaboradores em cibersegurança e de aumentar a consciencialização dos funcionários quanto ao tema.

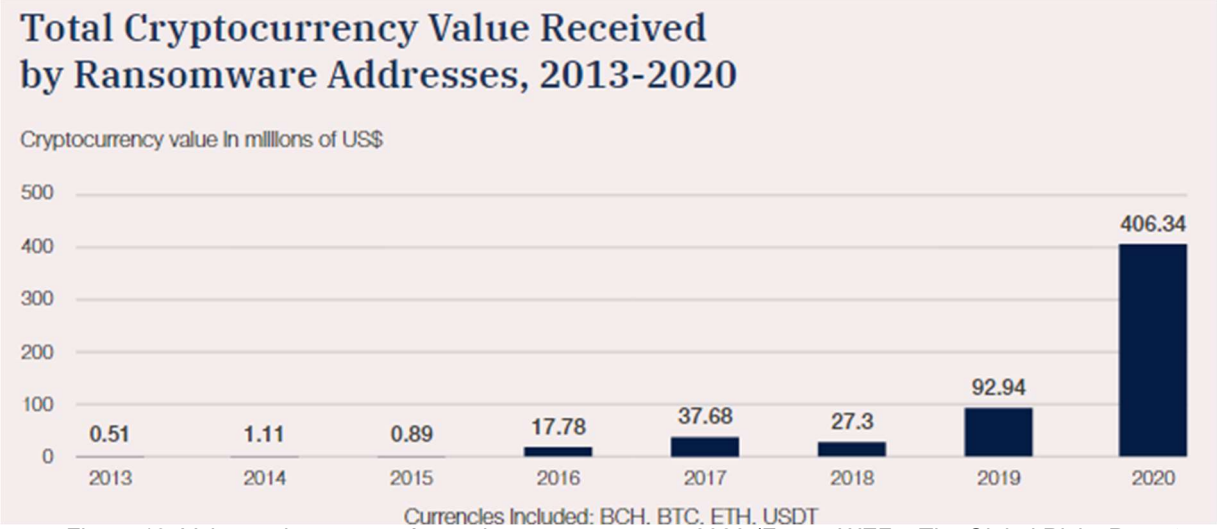

Figura 13: Valor total pago por vítmas de ransomware, em 2020 (Fonte: *WEF – The Global Risks Report – 2022 edition*)

O WEF (2022) ainda conclui que a dependência digital das empresas nas operações tem alavancado os resultados, mas por outro lado estão a expô-las a uma gama vasta de ataques que estão a ficar mais agressivos e abrangentes desde 2020, tornando o impacto maior. Os cibercriminosos estão a utilizar táticas mais elaboradas, como o uso de engenharia social com *deep fake*, direcionadas a alvos com vulnerabilidades expostas devido a facilidade de exploração e empresas tipicamente industriais e infraestrutura crítica se encaixam neste perfil.

3.3. Tendências para o cenário futuro

A nível nacional, a tendência é que as organizações sigam o mesmo passo e o estímulo seja alavancado pelos recentes ataques às empresas, como Vodafone e Germano de Sousa. A CNCS (2022) ressalta em seu relatório "Cibersegurança em Portugal – Riscos & Conflitos 2022" algumas das prospetivas de ciberameaças para 2022 e 2023 que podem impactar as organizações portuguesas, tanto na esfera pública quanto na privada:

- Incerteza sobre o contexto pandémico ou sobre a substituição deste contexto pelo do conflito na Ucrânia, onde cibercriminosos apoiados por entidades estatais desestabilizam economias e infraestruturas críticas gerando um impacto sistémico, especificamente no bem-estar de populações;
- Aumento de ciberameaças que exploram o fator humano seguirão a tendência mundial de utilizar as redes sociais, cripto moedas e plataformas de venda online como meios para explorar as fragilidades humanas para obter informações pessoais (PII), financeiras ou médicas, com intuito final que pode variar desde burla até venda das informações obtidas;
- Continuação do aumento dos incidentes de r*ansomware* deve ter destaques no futuro em curto-prazo devido a fragilidade tecnológica das empresas e a falta de preparo das pessoas quanto ao tema. *Ransomware-as-Service* é um derivado que tem se popularizado devido a facilidade atual em executar o ataque sem ter a infraestrutura ou conhecimento técnico necessário para tal, pois estas são "compradas" de quem as tem;
- Comprometimento de conta dos utilizadores para violação de dados continuará a ser um, ou o principal, modo de intrusão nos sistemas corporativos para vazamento de dados sensíveis e pessoais;
- Aumento da exploração de vulnerabilidades de sistemas de informação com o objetivo de penetrar e instalar códigos maliciosos que podem causar divulgação de informações restritas, diminuir a integridade de aplicações e indisponibilidade de serviços, ocasionando danos financeiros e reputacionais às organizações. Uma tendência para o futuro a curto-prazo quanto à vulnerabilidade é a agilidade na exploração de fragilidades *zero-day*, onde o alvo é uma fragilidade que a empresa ainda desconhece sua existência ou que descobriu muito recentemente, portanto o tempo entre a descoberta da vulnerabilidade pela organização e o seu uso como vetor de ataque pelo agente malicioso está cada vez menor, por isso é necessário que a empresa esteja atenta à sua superfície de exposição e em como deve agir para mitigar tais vulnerabilidades;

- A constante crescente da utilização de tecnologias móveis no dia-a-dia corporativo torna mais difícil a gestão de ativos e o uso de tecnologias emergentes como Internet das Coisas (*Internet of Things* - IoT), especialmente em ambiente industriais (*Industrial Internet of Things* – IIoT), aumenta a exposição da empresa aos ataques de grande impacto e de probabilidade.

Especificamente sobre as tendências futuras de recursos humanas em cibersegurança, o estudo da CyberEdge Group (2022) indica que a falta de profissionais qualificados continuará a ser um grande inibidor de sucesso nas organizações, devido a fatores como a rápida evolução tecnológica e falta de investimento da gestão. Essa escassez tem piorado e está cada vez mais claro que a oferta pode não acompanhar a demanda. Portanto, algumas perguntas devem ser feitas para alterar o *status quo*:

- Devem ser definidos os trabalhos de segurança para torná-los mais atraentes?
- É preciso fazer melhor uso de funcionários de meio período e *freelancers* para tarefas específicas?
- É preciso recrutar e treinar candidatos de grupos negligenciados?
- Devem ser executados programas de aprendizagem com escolas e faculdades locais?
- É preciso atrair a nova geração com jogos de realidade virtual e simulações de segurança cibernética?

Além de olhar para o ambiente externo, outra opção é olhar para o que já existe na organização e fazer melhor uso do que está disponível como automatizar tarefas de segurança para que os especialistas possam direcionar seu foco em trabalhos mais voltados a definições estratégicas, ou mesmo olhar para os colaboradores e identificar possíveis situações de formação para novos profissionais de segurança da informação e elevar as competências de profissionais já experientes (CyberEdge Group, 2022; p.58).

4. Metodologia

A tese tem como principal objetivo entender o estado atual da Cibersegurança em Portugal e como ela tem sido aplicada nas entidades públicas e privadas que atuam no país, portanto a metodologia utilizada foi um inquérito aberto ao público português através das mídias socias e contacto direto. O inquérito teve como referência o *2022 Cyberthreat Defense Report* do CyberEdge Group e o *ENISA Threat Landscape Report 2021* e é composto por perguntas de controlo sobre a organização, como quantidade de funcionários e o setor de atuação, além de três secções que auxiliam na perceção do perfil de cada resposta. As três secções são:

- Secção 1 – Maiores preocupações das organizações portuguesas: este segmento do inquérito tem como objetivo compreender quais são os tipos de preocupações atuais dentre as entidades portuguesas, que podem variar de fraude de pagamentos a roubo de credenciais e sequestro de dados. Para este último, que é a maior preocupação no país no campo da cibersegurança, também foram feitas questões quanto a decisão de pagar pelo resgate dos dados. Ainda nesta secção, também existem questões quanto ao orçamento da organização destinado à segurança da informação, quais aspetos mais afetam na defesa contra crimes cibernéticos e o nível em segurança da informação de determinados componentes tecnológicos.
- Secção 2 – Principais consequências da falta de segurança da informação: esta secção apresenta questões como a quantidade de ataques em um passado recente e a perceção para um futuro próximo, dificuldade em contratar determinadas posições laborais e a adequabilidade de algumas subáreas da SI face aos contextos externo e interno.
- Secção 3 – Ações para melhoria da postura em segurança da informação: Este último segmento do inquérito dispõe de questões relacionadas a ações concretas que visam a melhoria do perfil corporativo (postura) em SI, nomeadamente a utilização de uma referência internacional para definição de controlos de SI, práticas para aprimorar a segurança de aplicações web e aplicativos *mobile*, tecnologias e arquiteturas utilizadas para robustecer o teletrabalho e, novamente, sobre o orçamento para SI, desta vez com foco no futuro. No que toca a recursos humanos, esta secção identifica qual o tipo de certificação de competências é mais valioso atualmente para as organizações portuguesas.

O inquérito é uma amostragem por conveniência solicitado à cinquenta e seis empresas com presença no país e foi estruturado desta forma para alcançar o máximo possível de cenários existentes para cada organização de cada setor de atividade, permitindo que cada

resposta representasse fielmente as dificuldades, facilidades e projeções de futuro em SI de uma organização. Os resultados apresentados a seguir representam a participação efetiva entre Janeiro e Fevereiro de 2023 de vinte e oito líderes e gestores de organizações de diversos setores que possuem operações em Portugal, através de suas sucursais ou pela sua sede no país. O inquérito computou mais cinco participações incompletas de organizações que não avançaram após as questões sobre a localização, a quantidade de funcionários e o setor de atividade, portanto estas participações incompletas estão compreendidas apenas nos gráficos relacionados a essas três primeiras questões.

Esta secção do inquérito se dedica a identificar quais são as consequências de uma postura da organização que não implementa ou, no mínimo, não faz os investimentos necessários em segurança da informação. Para cada organização e setor de atividade, podem existir diferentes tipos de consequências, no entanto o inquérito seguiu a linha da ameaça cibernética pois esta é uma das principais causas de disrupção no negócio, logo, serão enfatizados os dados referentes a consequências causadas por *ransomware.*

O inquérito se encontra, na íntegra, no secção Anexo A desta tese.

5. Análise da situação das organizações portuguesas - Apresentação de Resultados

5.1. Caracterização das empresas respondentes

Do total de respostas obtidas, cerca de 66% são relativas a organizações que possuem apenas sucursais em Portugal (ou seja, têm a sua sede no estrangeiro), indicando uma relevante participação de entidades estrangeiras neste estudo.

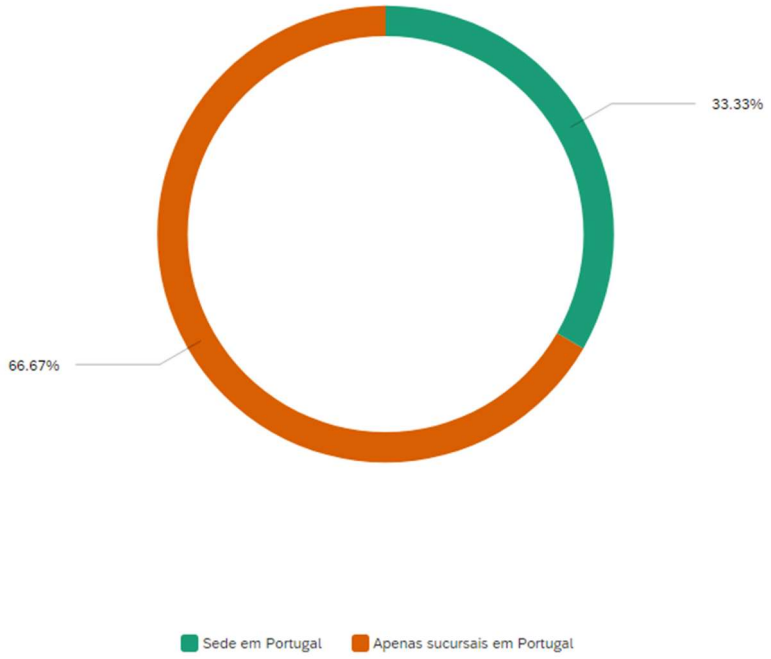

Figura 14: Empresas respondentes, por tipo de presença em Portugal (%)

Pelo facto do inquérito ter uma natureza direcionada para a tecnologia, houve um maior interesse das empresas que atuam em consultoria e no setor de Telecomunicações, seguida por setores extremamente regulados como os de Finanças e Seguros, Energia e outros serviços básicos como Água e Gás.

As participações dos setores Educação, Retalho, Saúde, Assistência Médica e Apoio Social, Administração e Serviços Públicos, bem como Agricultura foram solicitadas, no entanto estas participações não se concretizaram.

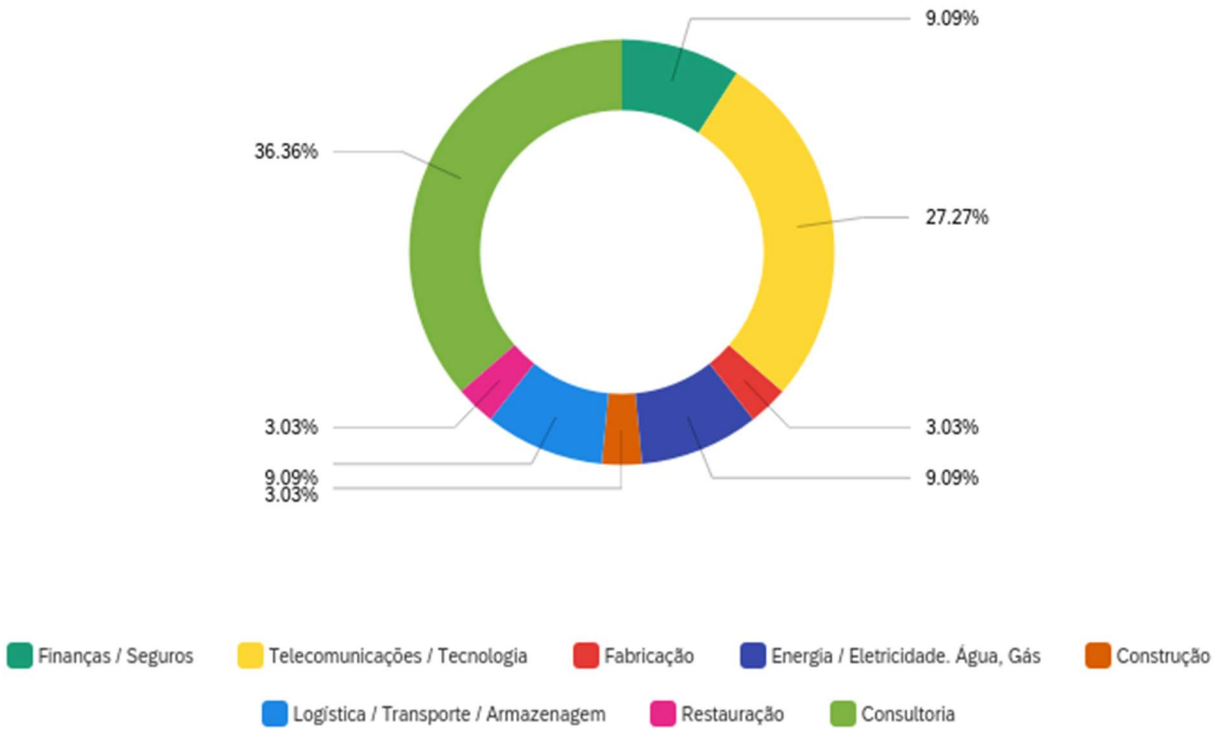

Figura 15: Empresas respondentes, por setor de atividade (%)

Devido ao número de respostas ter sido maior pelas organizações estrangeiras com sucursais em Portugal, que tipicamente possuem grande quantidade de funcionários, mais de metade das entidades respondentes têm entre mil e cinco mil funcionários ou mais de 5000 funcionários (Figura 16).

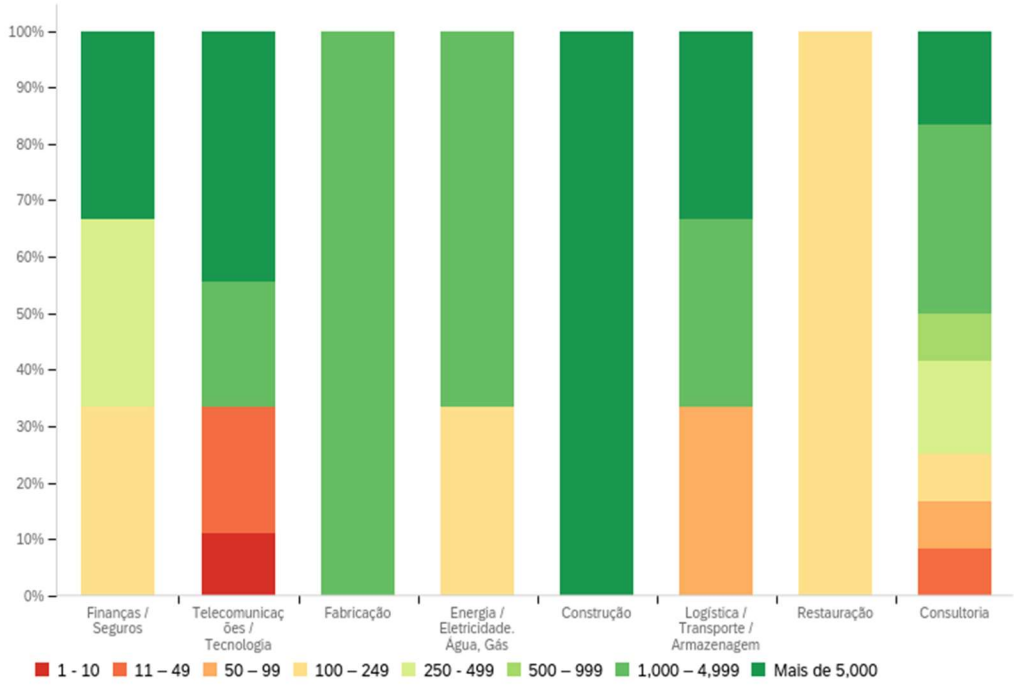

Figura 16: Respostas sobre quantidade de funcionários por presença em Portugal, em valores totais

5.2. Principais preocupações de Segurança da Informação

Na figura 17 é possível identificar que o ataque de sequestro de dados (r*ansomware*) é a ameaça que o maior número de respondentes considera como mais preocupante, seguida por outras ameaças de preocupação média para os participantes como a invasão de conta e abuso de credenciais, *phishing* e ataques à reputação nas redes sociais e na web, estando estas respostas alinhadas com os alertas de órgãos nacionais e estrangeiros como o CNCS e a ENISA, respetivamente.

De acordo com os respondentes, as ameaças menos preocupantes são as internas e os ataques *zero-day*. No primeiro caso, isto indica que os participantes não visualizam seus colaboradores como possíveis causadores de ataques à organização e, no segundo caso, não há o interesse ou a preocupação de encontrar vulnerabilidades que ainda não são publicamente conhecidas.

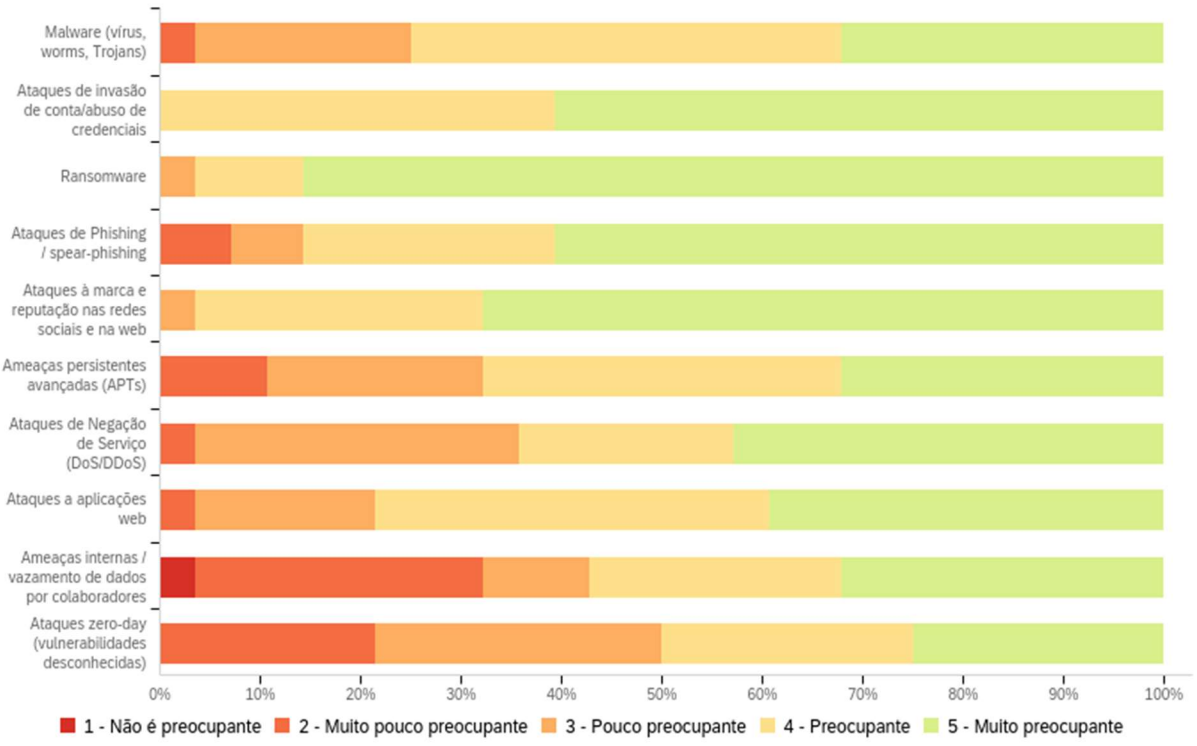

Figura 17: Nível de preocupação por tipo de ameaça cibernética

Ao olhar em detalhe para o *ransomware* e adicionando os setores de atuação ao gráfico, é possível perceber que esta ameaça é transversal dentre os diferentes setores de atividade das organizações respondentes. Isto indica que os participantes partilham da maior preocupação do país e do mundo, no âmbito da Segurança da Informação.

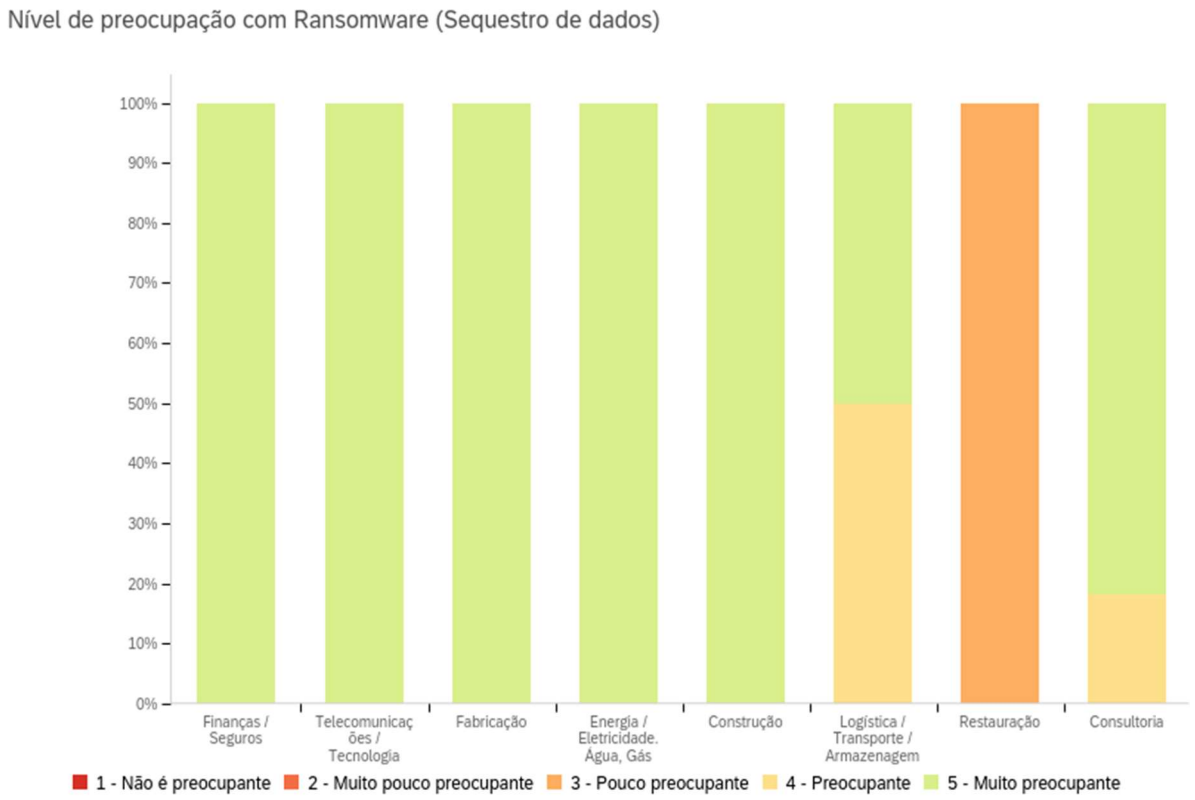

Figura 18: Nível de preocupação quanto ao *ransomware*, por setor de atividade

O *ransomware* tem como principal característica criptografar os dados da organização e requisitar pagamento para tê-los de volta, portanto os participantes também foram questionados se foram alvos deste tipo de ataque nos últimos 12 meses. As respostas na Figura 19 indicam uma maturidade dos participantes na prevenção, ou seja, não foram alvos deste ataque, assim como na recuperação, ou seja, na reposição dos dados previamente armazenados em outro local e que consequentemente elimina a necessidade de pagamento. Pelo facto de que nenhuma organização teve de pagar pelo resgate dos dados, pode concluir-se que há uma consciencialização das organizações portuguesas e das estrangeiras que atuam no país quanto ao perigo que é o *ransomware*.

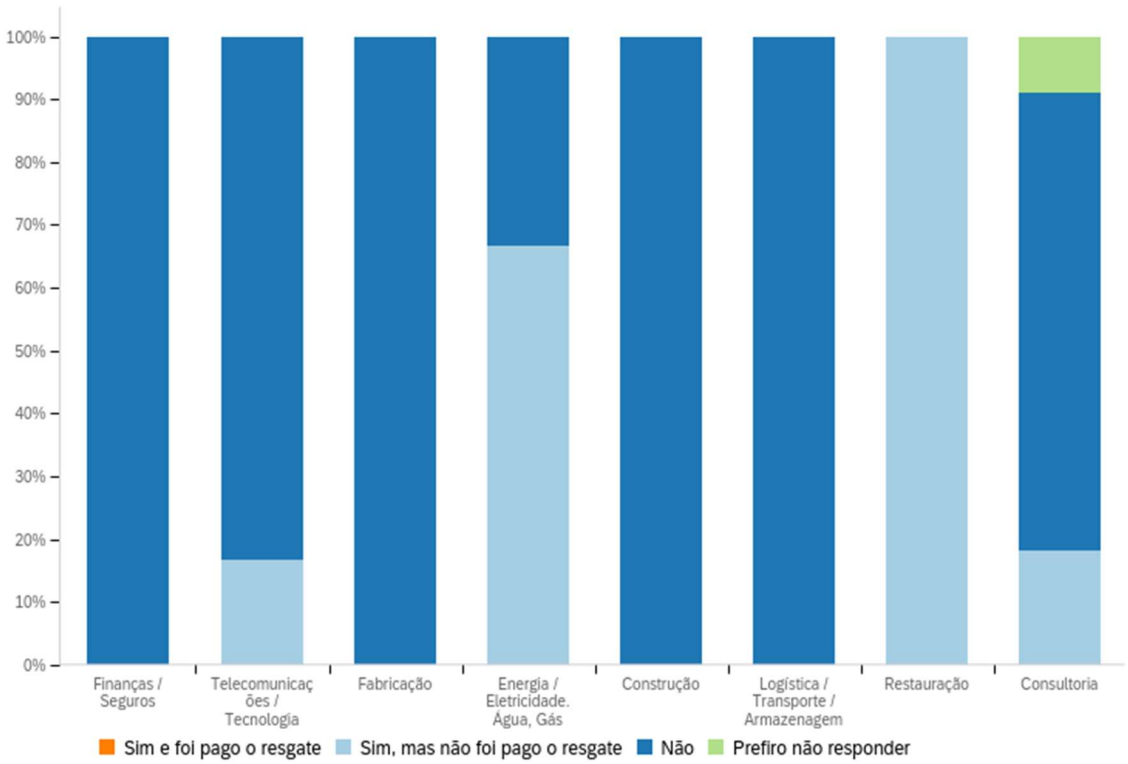

Figura 19: Indicador de ataque de *ransomware*, por setor de atividade

Sobre as ameaças menos preocupantes de acordo com os respondentes, a distribuição das respostas por setor de atividade é demonstrada nas Figuras 20 e 21. As respostas indicam que mesmo as empresas respondentes de setores com obrigações legais elevadas, tanto por legislações nacionais do próprio setor quanto diretivas internacionais, como é o caso do conjunto de setores de atividade em Energia, Eletricidade, Água e Gás, não consideram estas ameaças como algo preocupante.

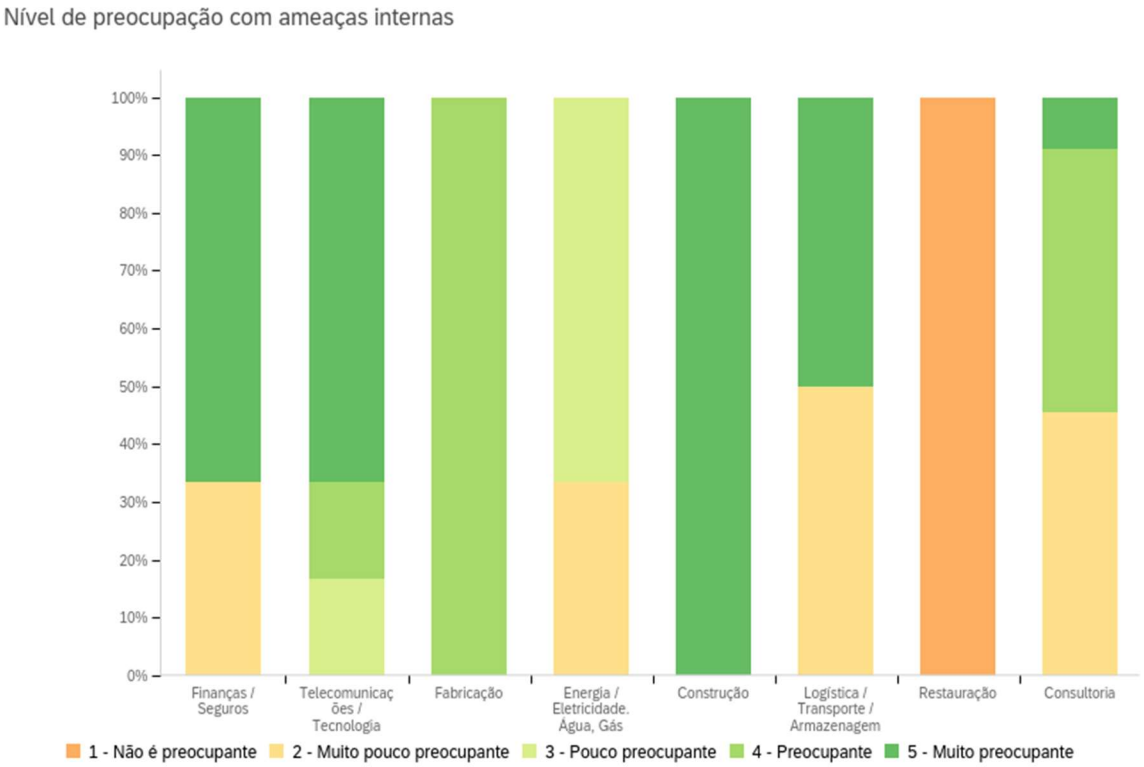

Figura 20: Nível de preocupação para ameaças internas, por setor de atividade.

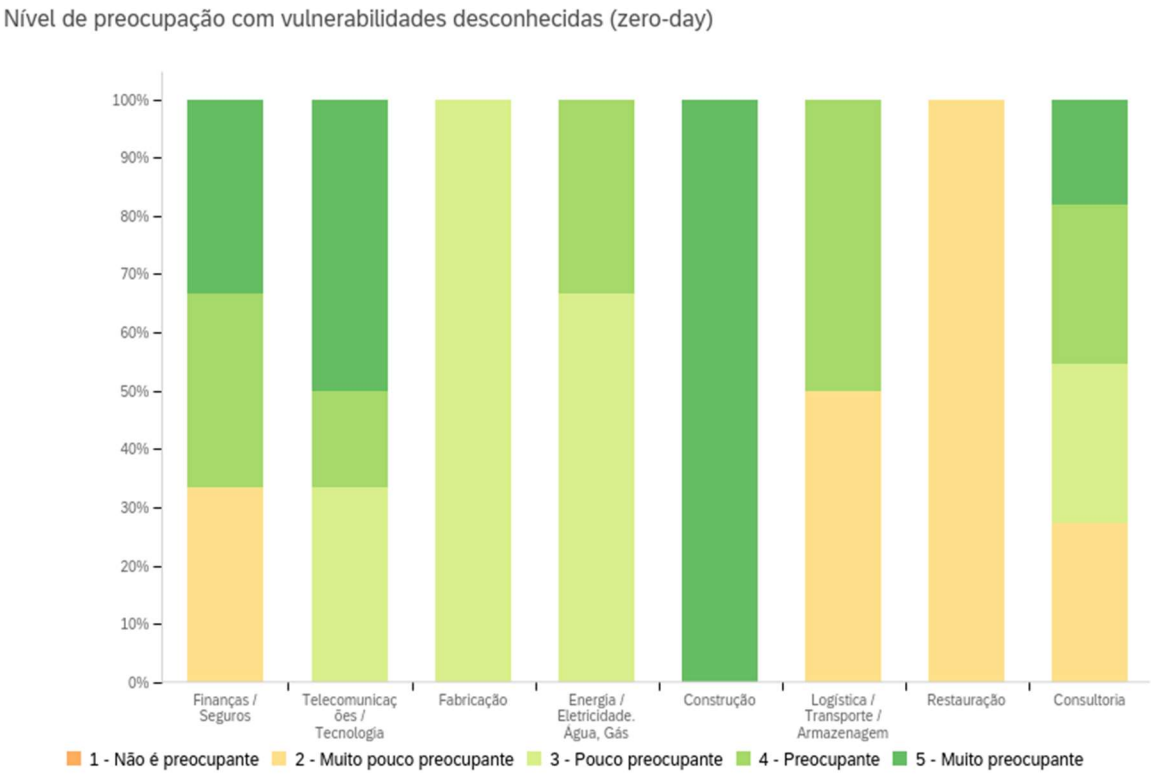

Figura 21: Nível de preocupação para a ameaça *zero-day*, por setor de atividade

Os respondentes foram também inquiridos sobre quais as ameaças a aplicações web e *mobile* que são preocupantes para o setor em que atuam. De acordo com as respostas, os

respondentes preocupam-se com roubo de credenciais e recolha de dados pessoais indevida, este último devido ao risco de sanções previstas no RGPD. Há uma pequena percentagem quanto ao ataque de negação de inventário que, em outras palavras, se trata de um ataque com objetivo de impedir que a organização aceda ao seu próprio inventário, criando assim uma disrupção nas operações da organização.

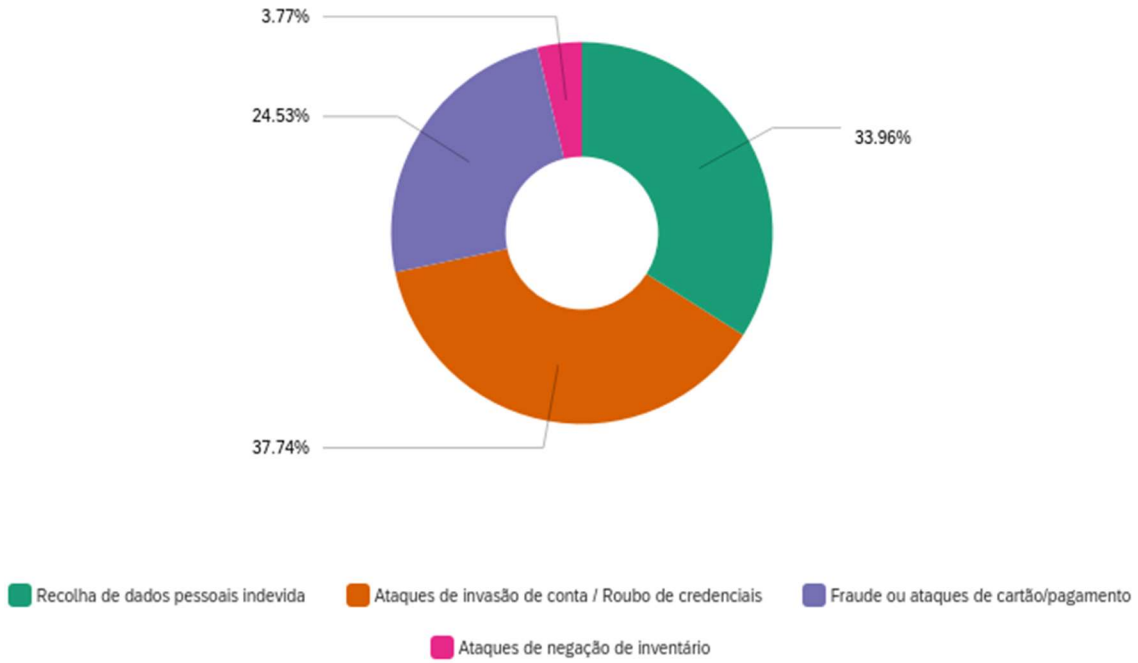

Figura 22:Tipos de ataques às aplicações web e *mobile* preocupantes, por setor de atividade, em percentagem

Os respondentes também foram questionados sobre qual é o nível de impacto na organização que os seguintes aspetos possuem na defesa contra ameaças cibernéticas:

- Falta de profissionais qualificados;
- Baixa consciencialização de segurança da informação entre os colaboradores;
- Fraca interoperabilidade entre soluções de segurança da informação;
- Falta de suporte ou consciencialização da gestão;
- Muito dados para serem analisados.

As Figuras 23 a 25 indicam quais são os aspetos de maior impacto nas organizações respondentes do inquérito. Dentre os três aspetos, dois deles são referentes a falta ou baixa consciencialização *top-down* e *bottom-up* do tema segurança da informação, especificamente na defesa contra as ameaças cibernéticas. O outro é referente a falta de profissionais qualificados no mercado laboral.

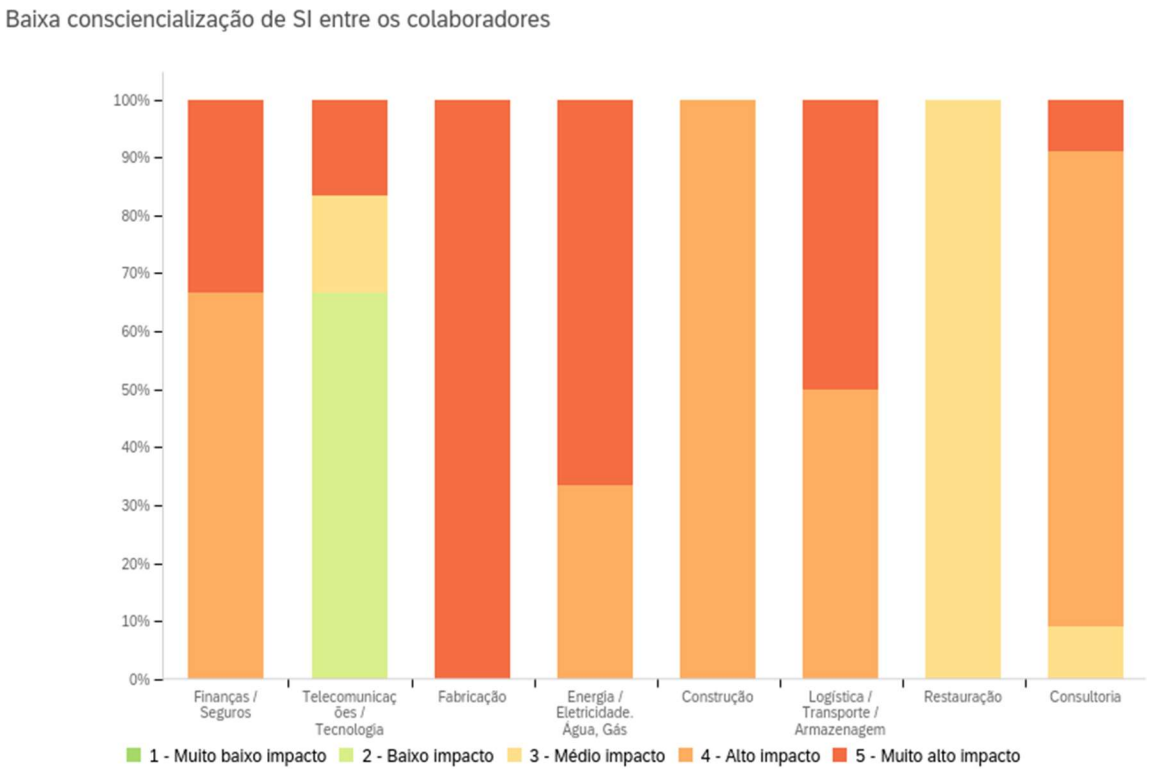

Figura 23: Nível de impacto da consciencialização entre colaboradores, por setor de atividade (%)

Com exceção ao setor de Telecomunicações, é possível perceber que a consciencialização, seja ela *top-down* ou *bottom-up*, é um tema que possui alto ou muito alto impacto de forma transversal para os demais setores. No caso do setor de Telecomunicações, um terço respondeu como baixo impacto a falta de suporte da gestão, ou seja, *top-down* (Figura 24) e dois terços entre os demais colaboradores (Figura 23).

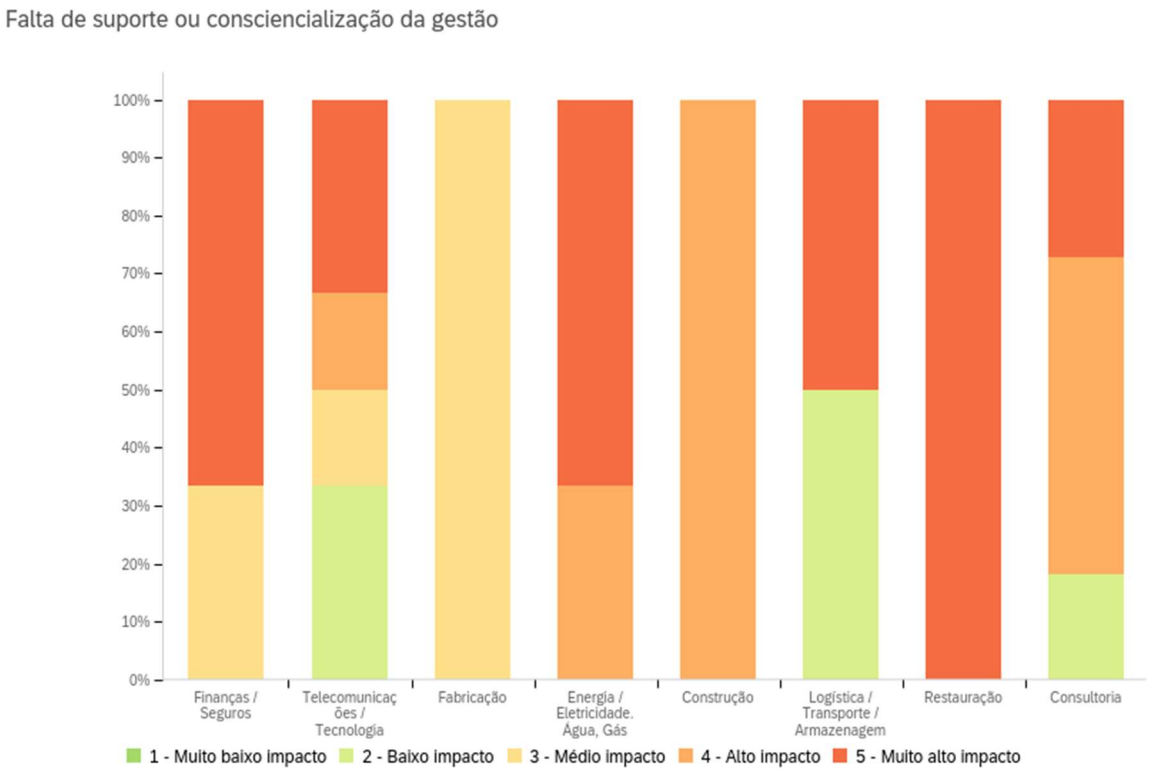

Figura 24:Nível de impacto da consciencialização na gestão, por setor de atividade (%)

O aspeto que mais foi referido por ter maior impacto na organização foi a falta de profissionais qualificados, estando em linha com o relatório "Cibersegurança em Portugal – Economia 2022", da entidade CNCS. Vale ressaltar que todos os setores de Finanças e Seguros, Energia e demais serviços básicos, Logística, Transporte e Armazenagem, bem como a Restauração, indicaram este aspeto como muito alto impacto. Além disso, outro ponto importante é que 60% dos respondentes do setor de Consultoria também indicaram este aspeto como muito alto impacto. Por outro lado, a exceção fica novamente a cargo do setor de Telecomunicações com um terço dos participantes a dizer que a falta de profissionais qualificados possui baixo impacto (Figura 25).

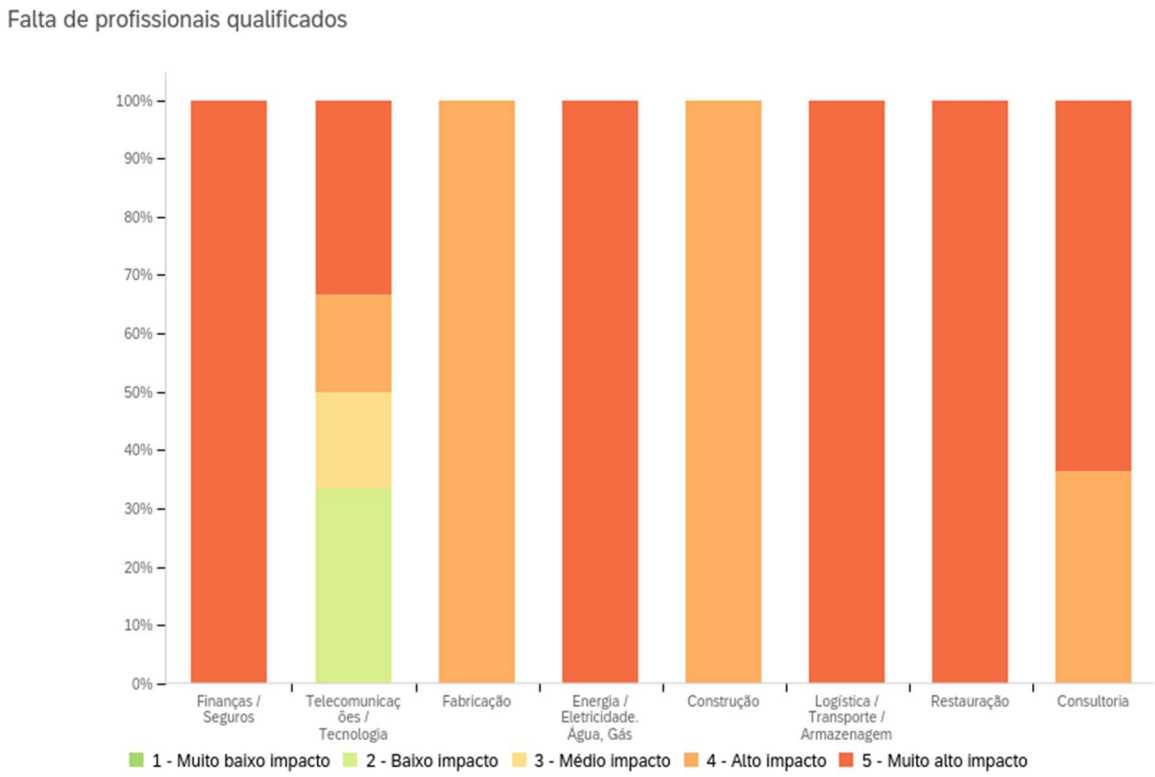

Figura 25:Nível de impacto da falta de profissionais, por setor de atividade (%)

Os participantes foram também questionados sobre quais os cargos que a organização tem dificuldade em encontrar profissionais qualificados. Nessa questão, onde foi possível escolher um ou mais cargos, cerca de 26,8% respondeu que o cargo de Gestor de SI atualmente é o mais difícil de encontrar profissionais qualificados, seguido por "Administrador/Analista/Consutlor de SI" e "Arquiteto/Engenheiro de SI", com 14,9% e 13,4%, respetivamente.

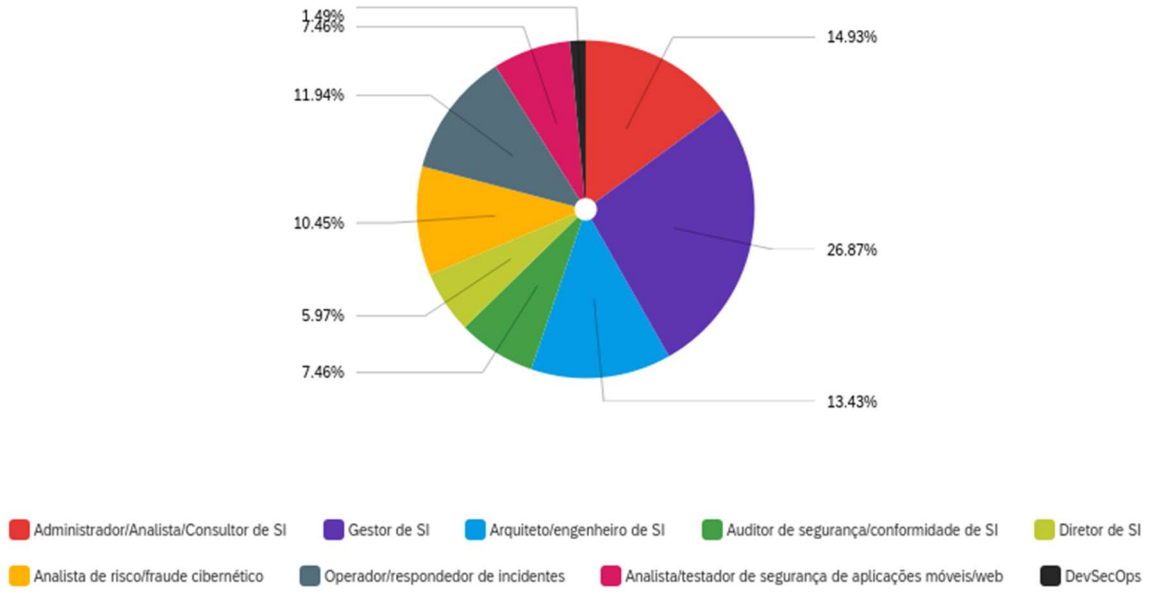

Figura 26: Cargos que são difíceis de encontrar profissionais qualificados, em percentagem

Os respondentes também foram questionados sobre qual é a percentagem do investimento em Tecnologias da Informação destinada aos projetos e iniciativas em Segurança da Informação. Como é possível perceber na Figura 27, é transversal a utilização de 0% a 5% do orçamento em tecnologia para os objetivos de segurança da informação.

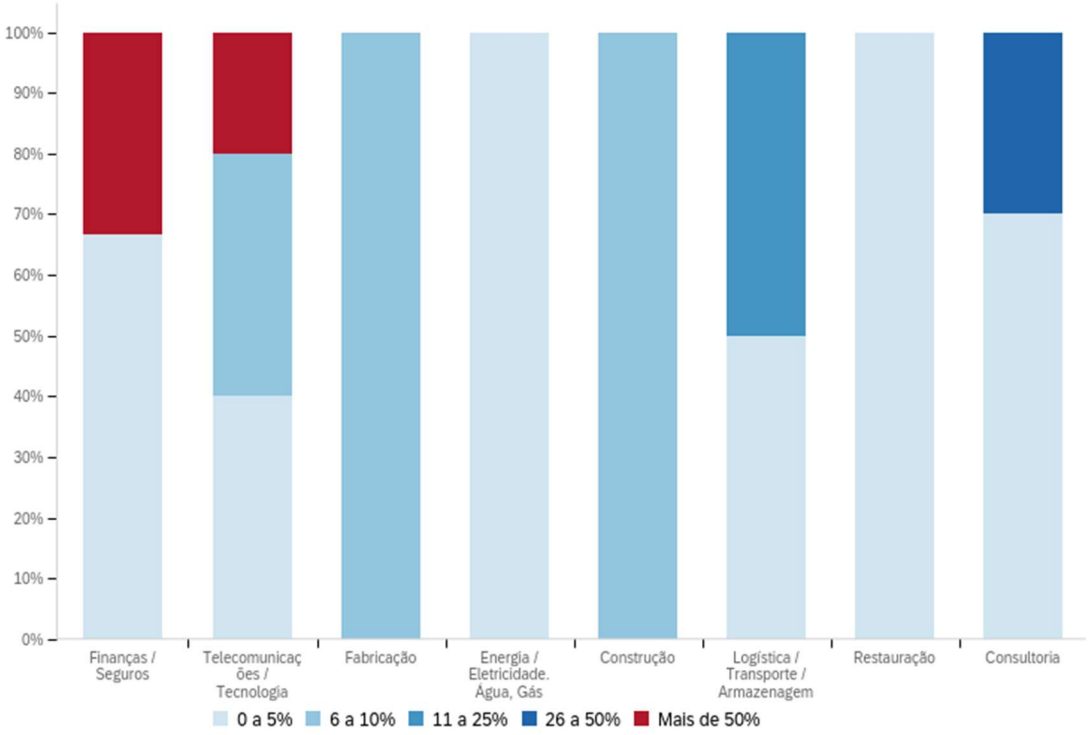

Figura 27: Percentagem do investimento destinado a SI, por setor de atividade (%)

Quando a mesma questão é observada sob a perspetiva dos ataques de *ransomware*, é possível identificar que apenas as organizações que investem entre 0% a 5% em SI foram alvos deste ataque nos últimos 12 meses (Figura 28).

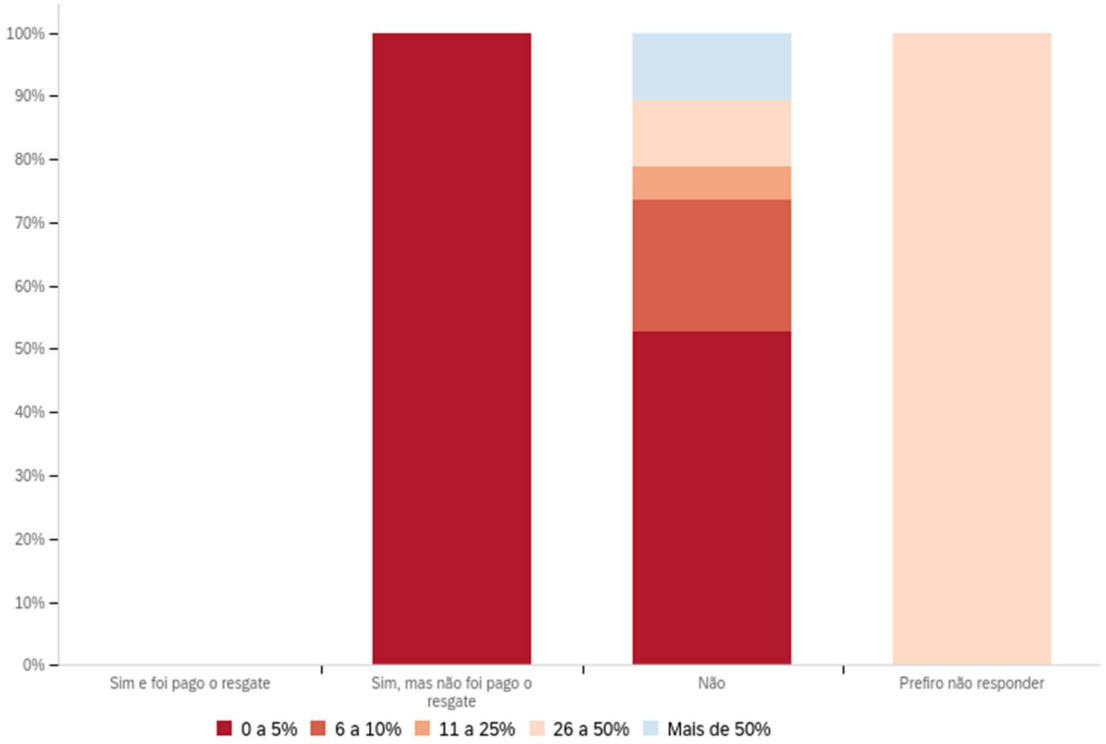

Figura 28: Relação percentagem de investimento em SI e ataques de *ransomware*

Com isso, é possível identificar que as principais preocupações das organizações participantes neste estudo para o tema Segurança da Informação são:

- A dificuldade de encontrar gestores, consultores, arquitetos, engenheiros, administradores e analistas tem origem na falta de profissionais qualificados no país;
- Os setores de atividades que foram alvos de ataque de *ransomware* possuem dificuldade em encontrar profissionais qualificados para os cargos mais operacionais, em destaque são os setores de Telecomunicações (77,8%), Energia e outros serviços básicos (70%) e Consultoria (59,4%);
- A falta de suporte *top-down* gera baixo investimento na área de segurança da informação e, aliado a isto, a falta ou baixa conscienciali*z*ação *bottom-up* deste tema gera preocupações com certas ameaças cibernéticas, como ataques a aplicações web e *mobile* que visam, sobretudo, o roubo de credenciais, de dados pessoais e fraudes nas transações financeiras.

5.3. Principais consequências da falta de Segurança da Informação

Nas Figura 29 a 33 são representadas as respostas quanto ao nível de segurança das soluções tecnológicas da organização sobreposto com a quantidade de ataques sofridos pela organização nos últimos 12 meses. Vale ressaltar que a maioria dos participantes consideram as suas soluções tecnológicas como seguras e mesmo assim indicam que foram alvo de um ataque entre uma a cinco vezes.

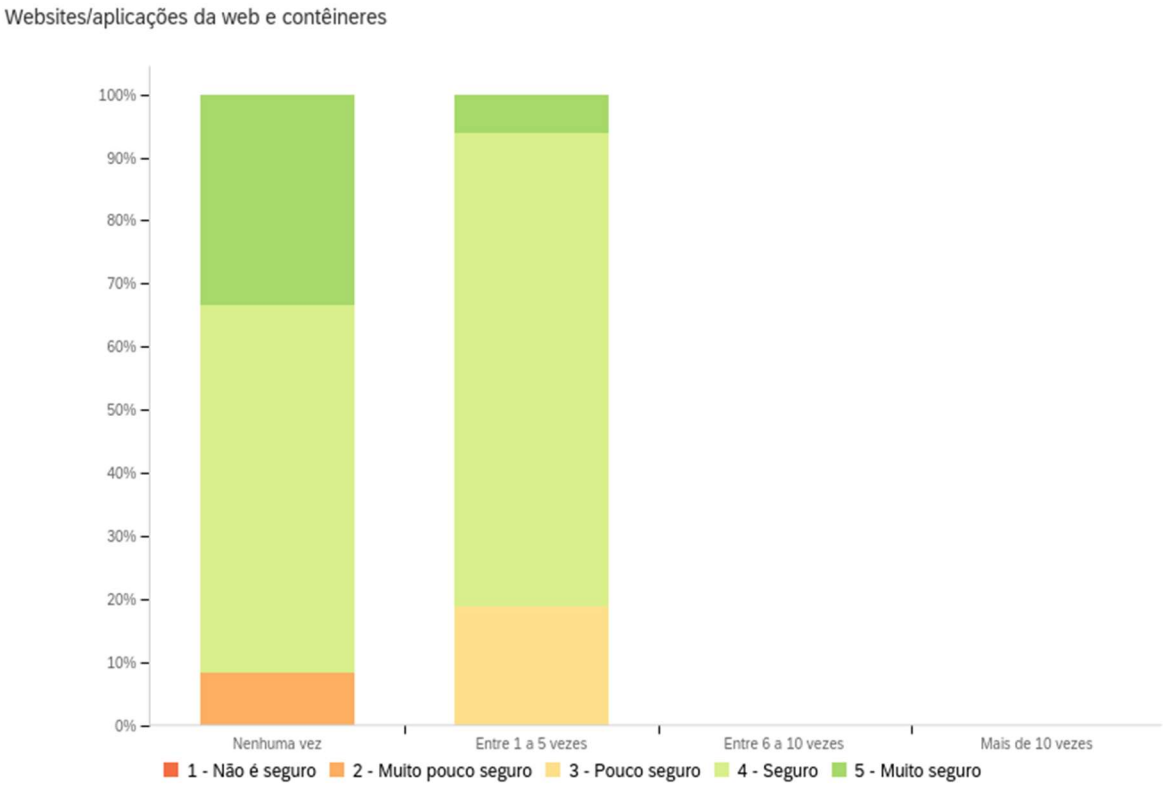

Figura 29: Relação quantidade de ataques sofridos nos últimos 12 meses e nível de segurança de soluções web, em percentagem

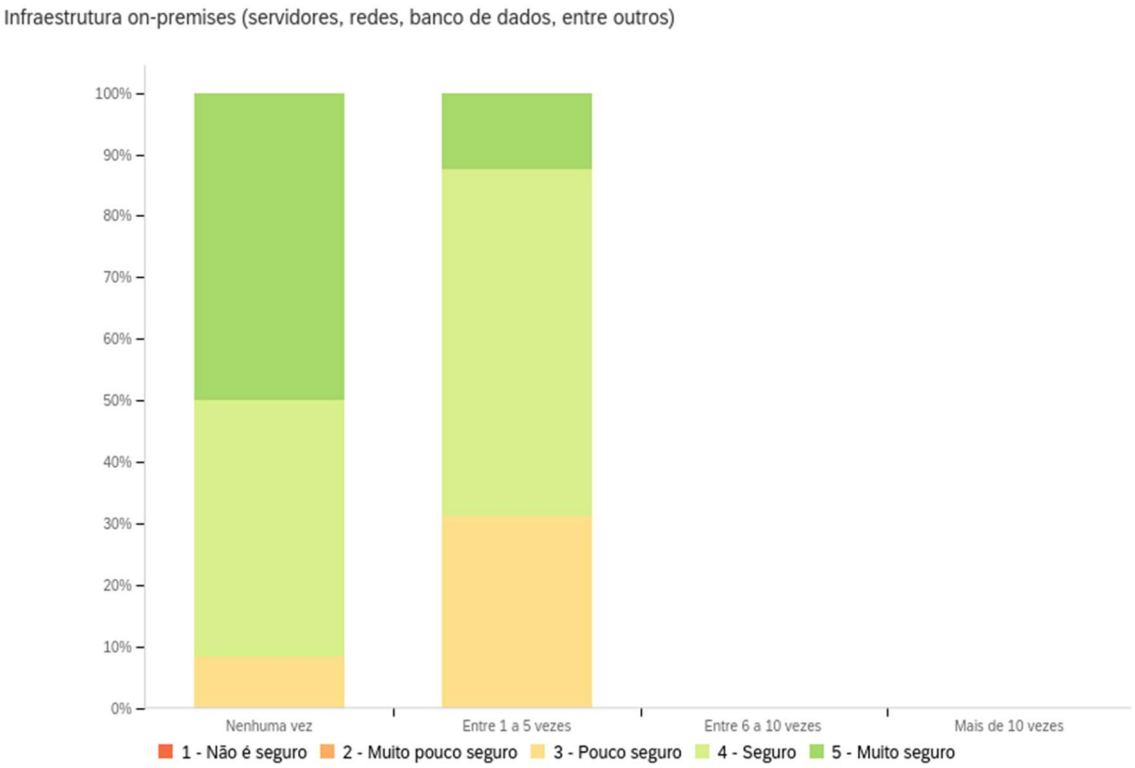

Figura 30: Relação quantidade de ataques sofridos nos últimos 12 meses e nível de segurança de infraestrutura *on-premises*, em percentagem

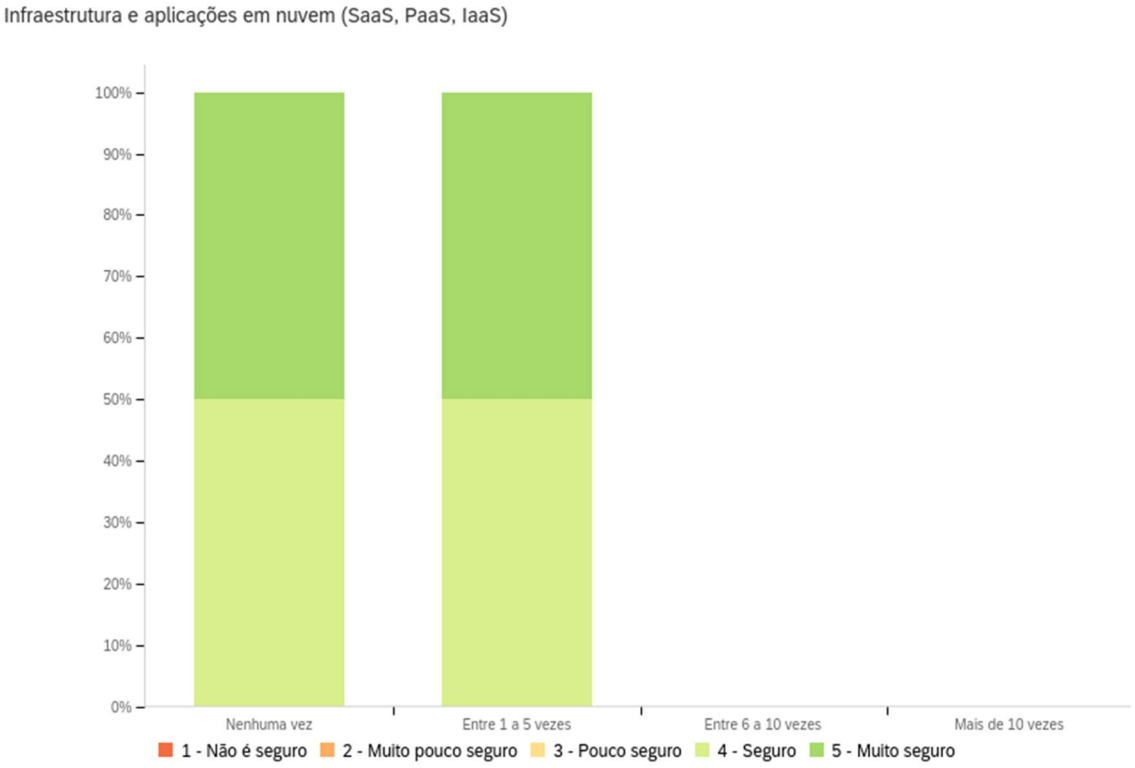

Figura 31: Relação quantidade de ataques sofridos nos últimos 12 meses e nível de segurança de infraestrutura em nuvem, em percentagem

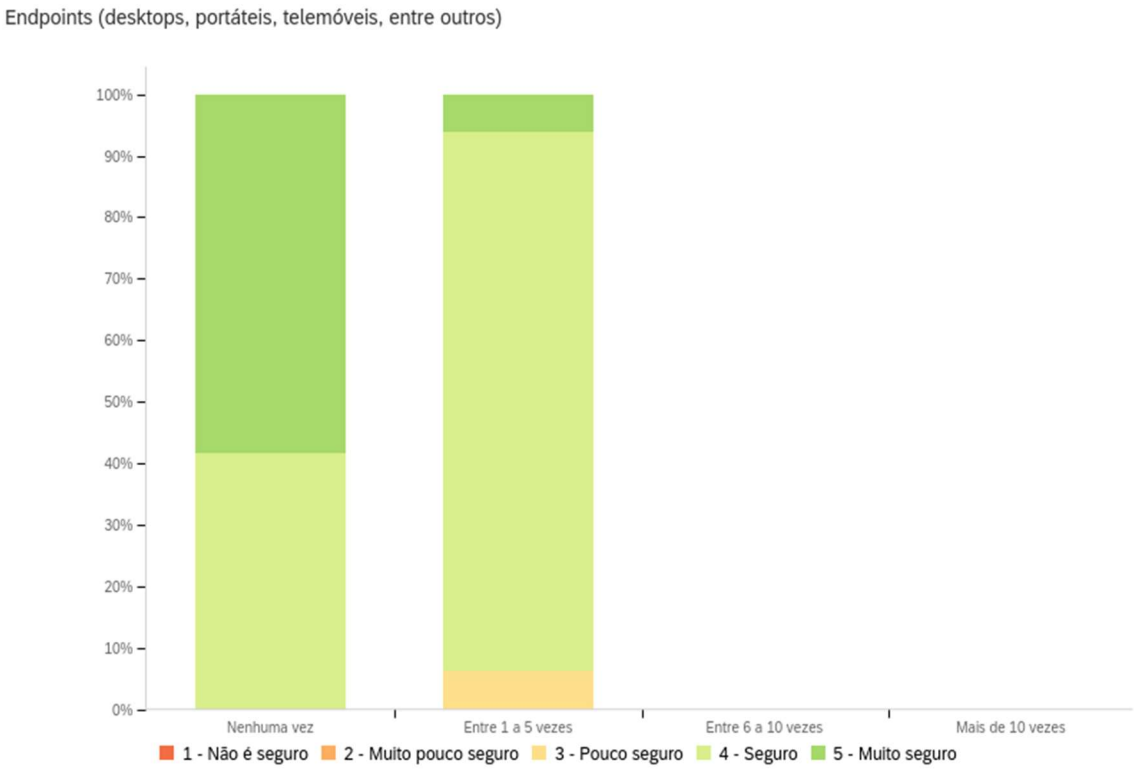

Figura 32: Relação quantidade de ataques sofridos nos últimos 12 meses e nível de segurança de *endpoints*, em percentagem

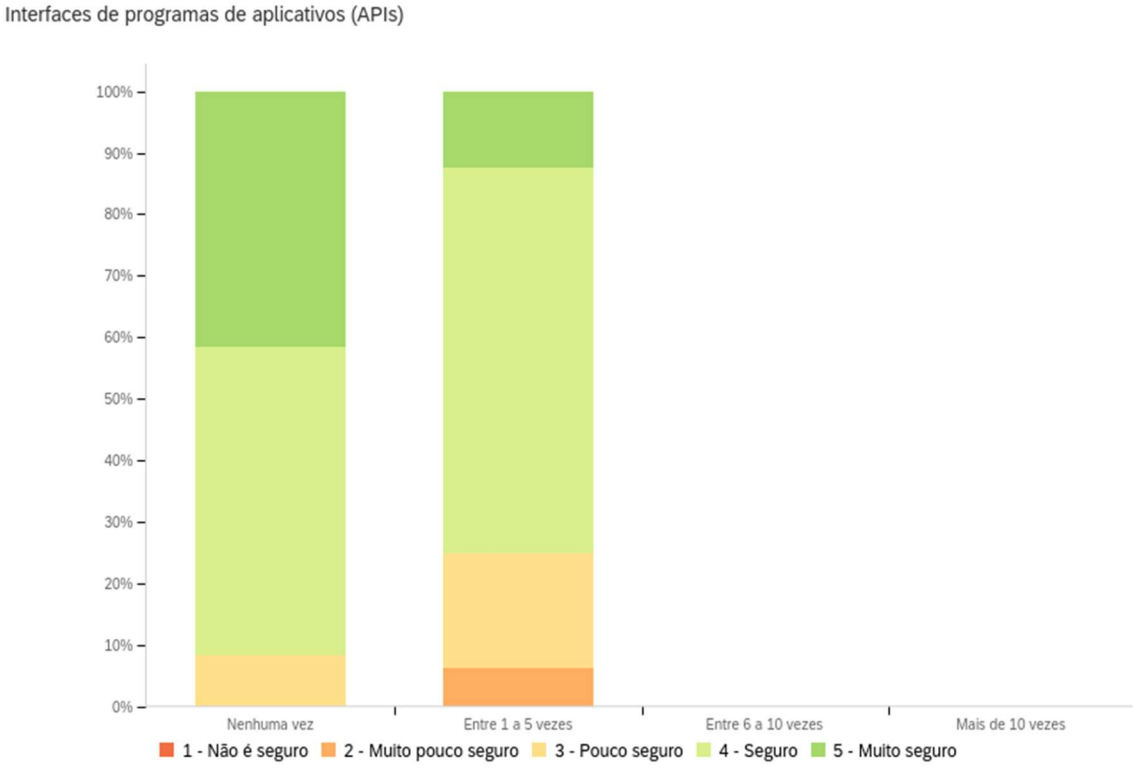

Figura 33: Relação quantidade de ataques sofridos nos últimos 12 meses e nível de segurança de *API*, em percentagem

Além de saber a quantidade de ataques sofridos nos últimos 12 meses, os participantes também tiveram de responder qual era a possibilidade de um ataque ocorrer nos próximos 12 meses. Quando estas duas questões são sobrepostas é possível perceber que, dentre as organizações que foram alvo, a possibilidade indicada é “Baixa” ou “Possível”, representando 55.5% e 78,6%, respetivamente.

As Figuras 34 e 35 mostram, respetivamente, essa sobreposição por tempo (passado e futuro) e por setor de atividade da organização.

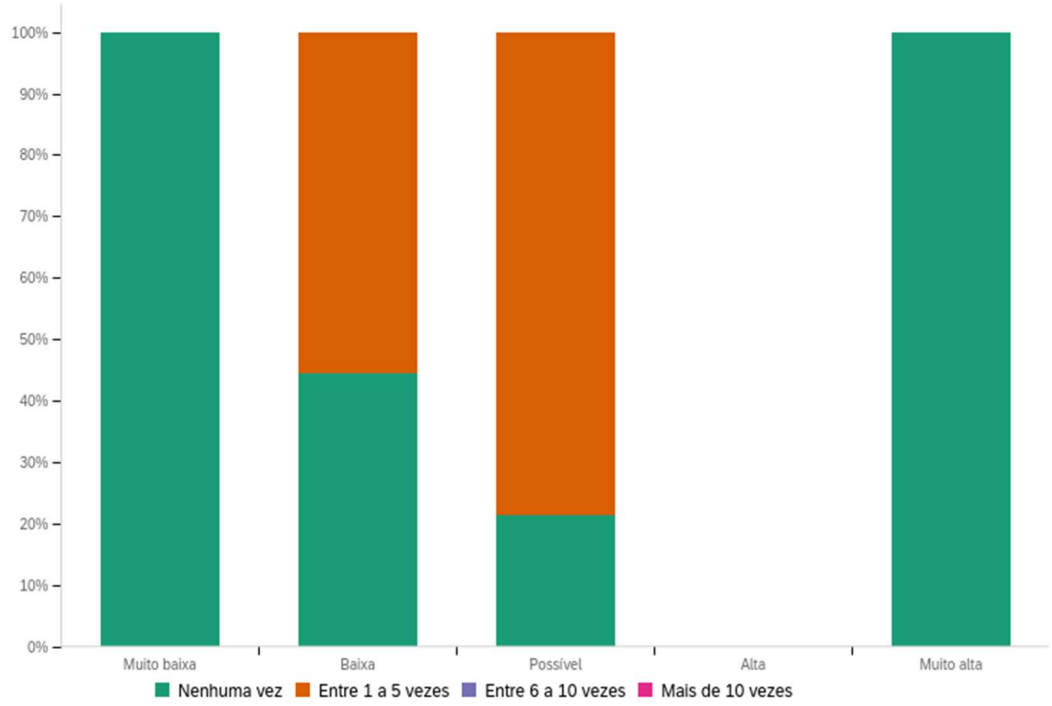

Figura 34: Relação ataques sofridos nos últimos 12 meses e possibilidade de ataques nos próximos 12 meses

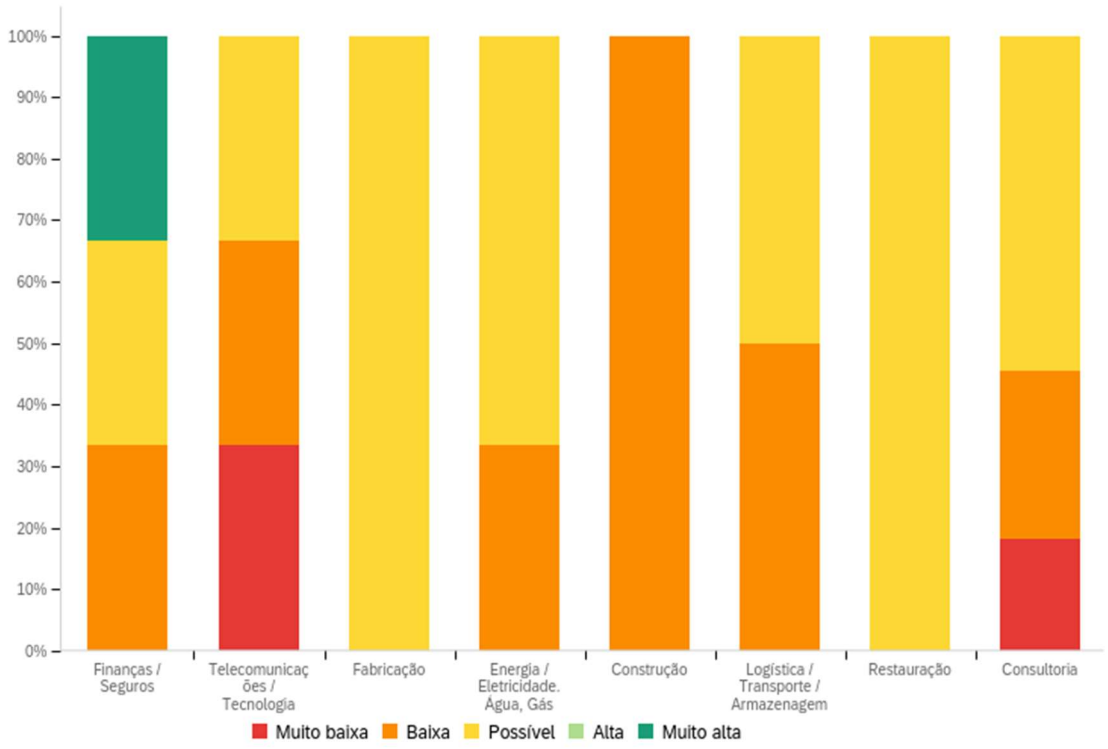

Figura 35: Possibilidade de ataques nos próximos 12 meses por setor de atividade (%)

Ao olhar especificamente para o ataque ransomware, independente da perceção de ataque nos próximos 12 meses, os participantes indicam que o ransomware é algo muito preocupante (Figura 36).

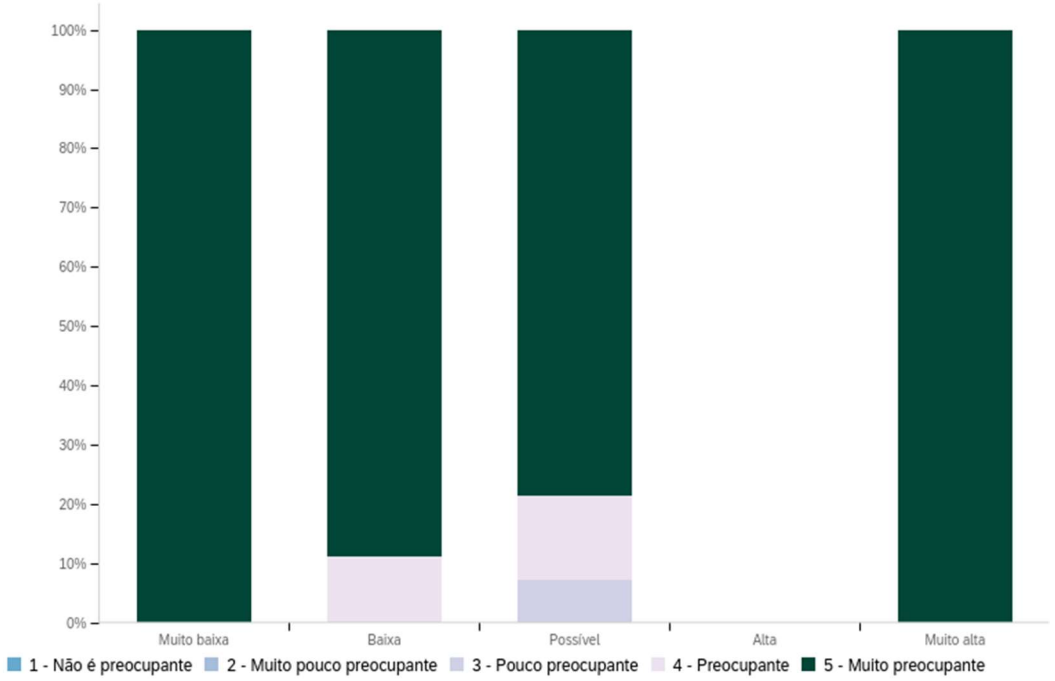

Figura 36: Relação nível de preocupação com ransomware e possibilidade de ataque nos próximos 12 meses

Outro ponto interessante de se observar são os respondentes que de facto sofreram este ataque e sua perceção face aos próximos 12 meses. Dentre os participantes que responderam “Sim” se já foram alvos, cerca de 70% acreditam ser possível que um novo ataque ocorra, enquanto os demais acreditam que exista uma baixa probabilidade de que tal evento ocorra novamente (Figura 37).

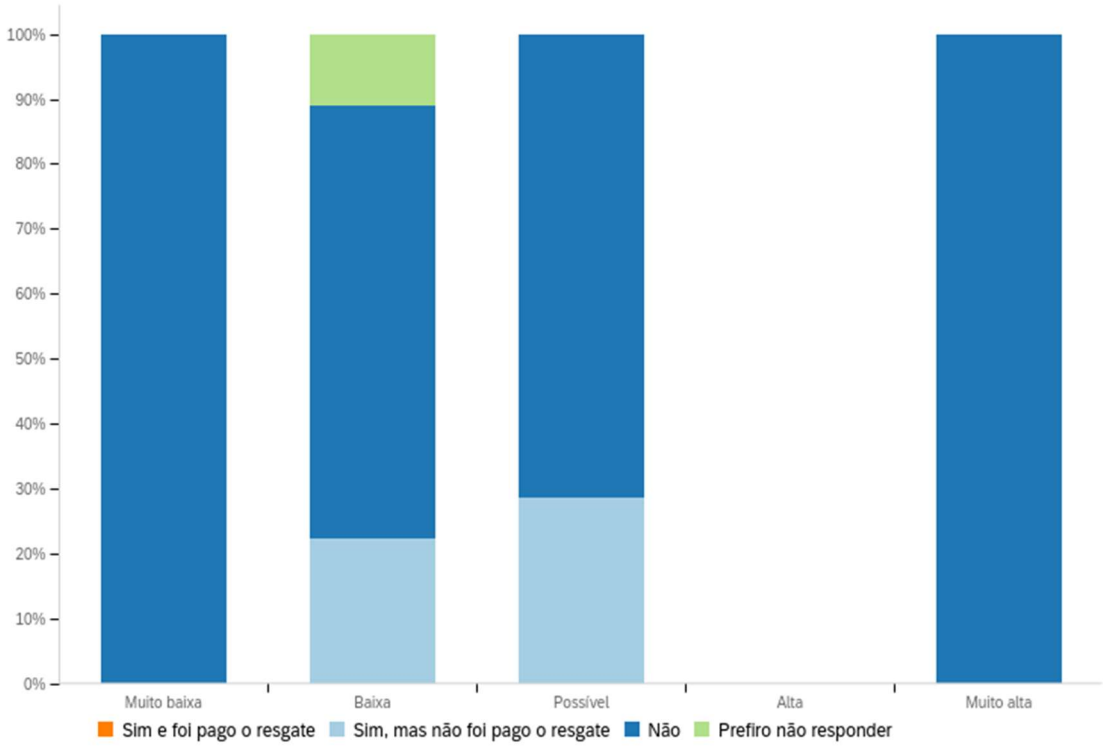

Figura 37: Participantes alvos de ransomware e sua perceção face aos próximos 12 meses

Os participantes também foram questionados sobre o nível de adequação face as necessidades que a organização possui, em sete subáreas da segurança da informação:

- Governança, risco e conformidade;
- Gestão de identidade e acesso;
- Deteção de ameaças avançadas e sofisticadas;
- Desenvolvimento seguro de software
- DevSecOps;
- Investigação e resposta a incidentes;
- Redução da superfície de ataque.

As Figuras 38 a 40 demonstram que há uma postura adequada de forma transversal em GRC, gestão do acesso e respostas a incidentes, que respetivamente tratam da governança de SI além da gestão de riscos da área e conformidade com obrigações legais aplicáveis à

organização, o outro no controlo ao acesso aos dados da organização e o último, na recuperação a um incidente de SI.

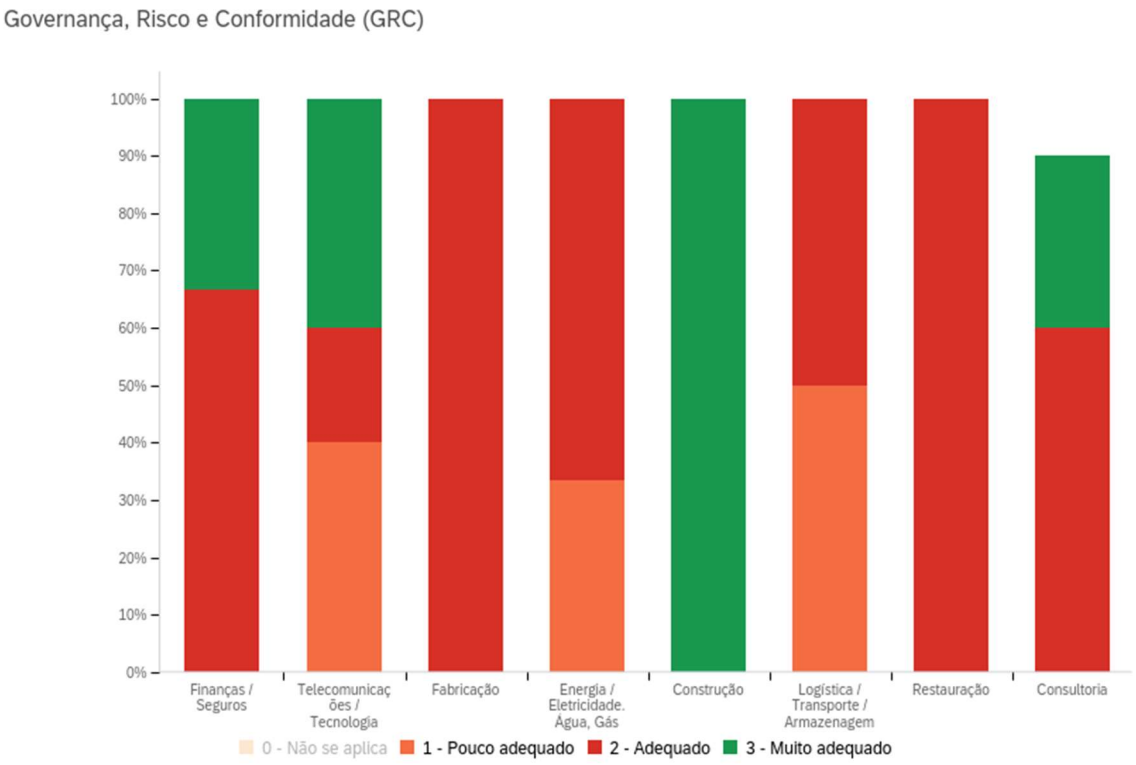

Figura 38: Nível de adequação em GRC, por setor de atividade

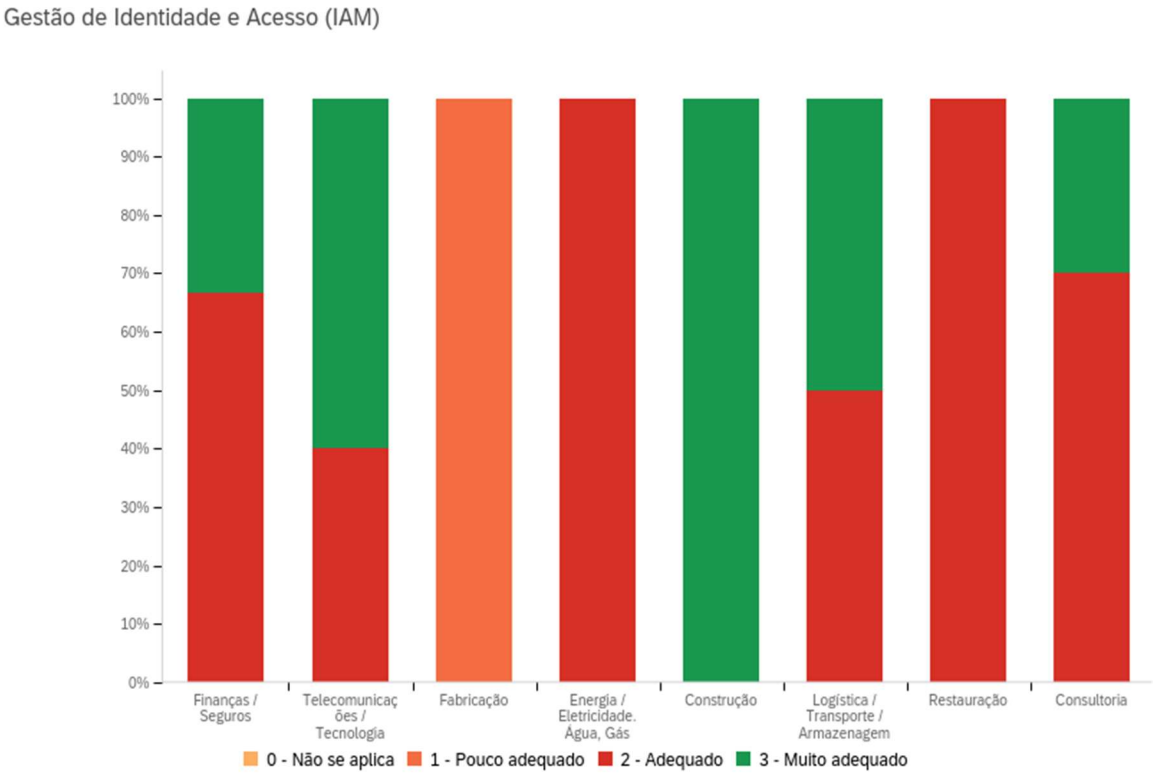

Figura 39: Nível de adequação em gestão de identidade e acesso, por setor de atividade

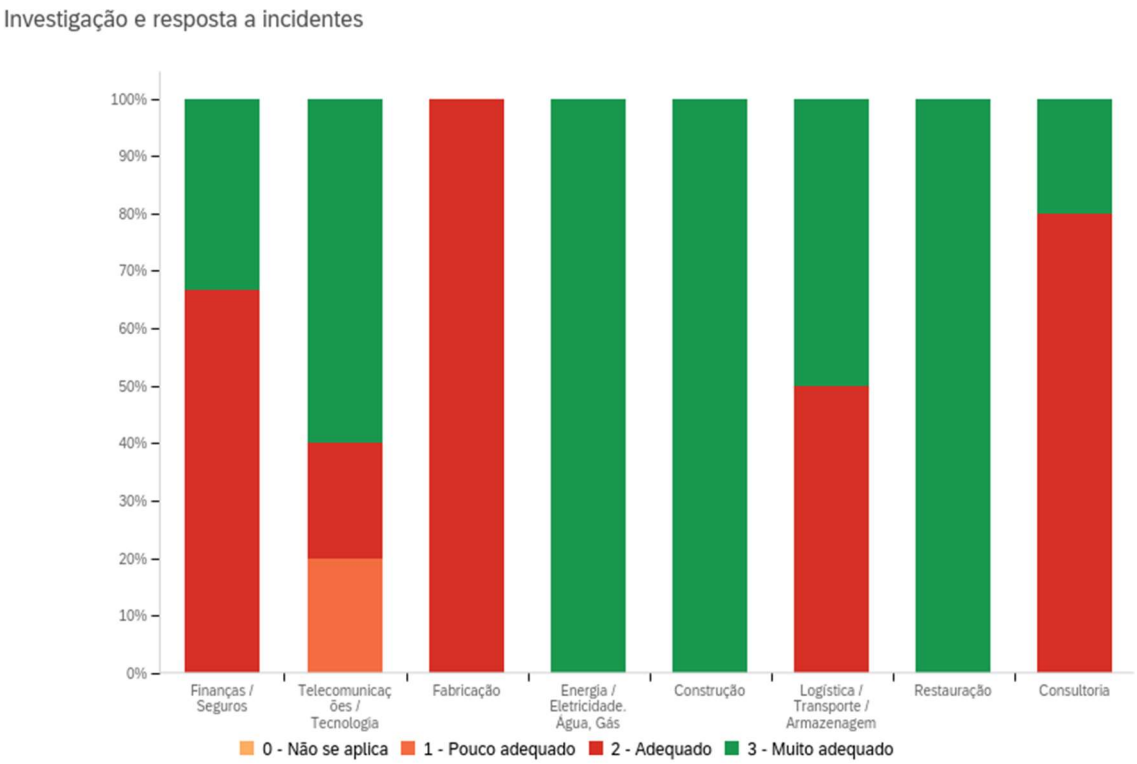

Figura 40: Nível de adequação para investigação e resposta a incidentes, por setor de atividade

Nas subáreas de redução de superfície de ataque, que trata da redução da exposição da organização face as ameaças cibernéticas, e deteção de ameaças sofisticadas, grande parte dos participantes indicam ter uma postura pouco adequada quando observada sob a ótica das necessidades da empresa (Figura 41).

Já nas subáreas “Desenvolvimento seguro de software” e “DevSecOps”, houve pouca aplicabilidade dentre os participantes, portanto quase a totalidade marcou a opção “Não se aplica”.

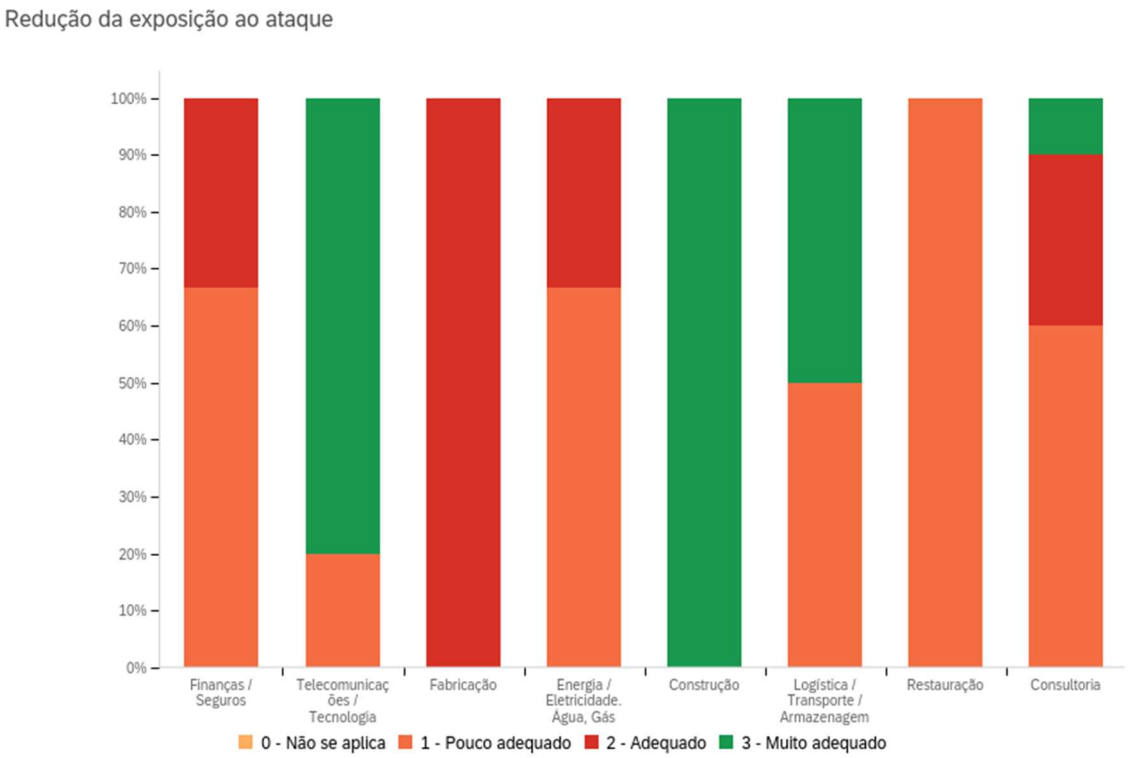

Figura 41: Nível de adequação para redução da superfície de ataque, por setor de atividade

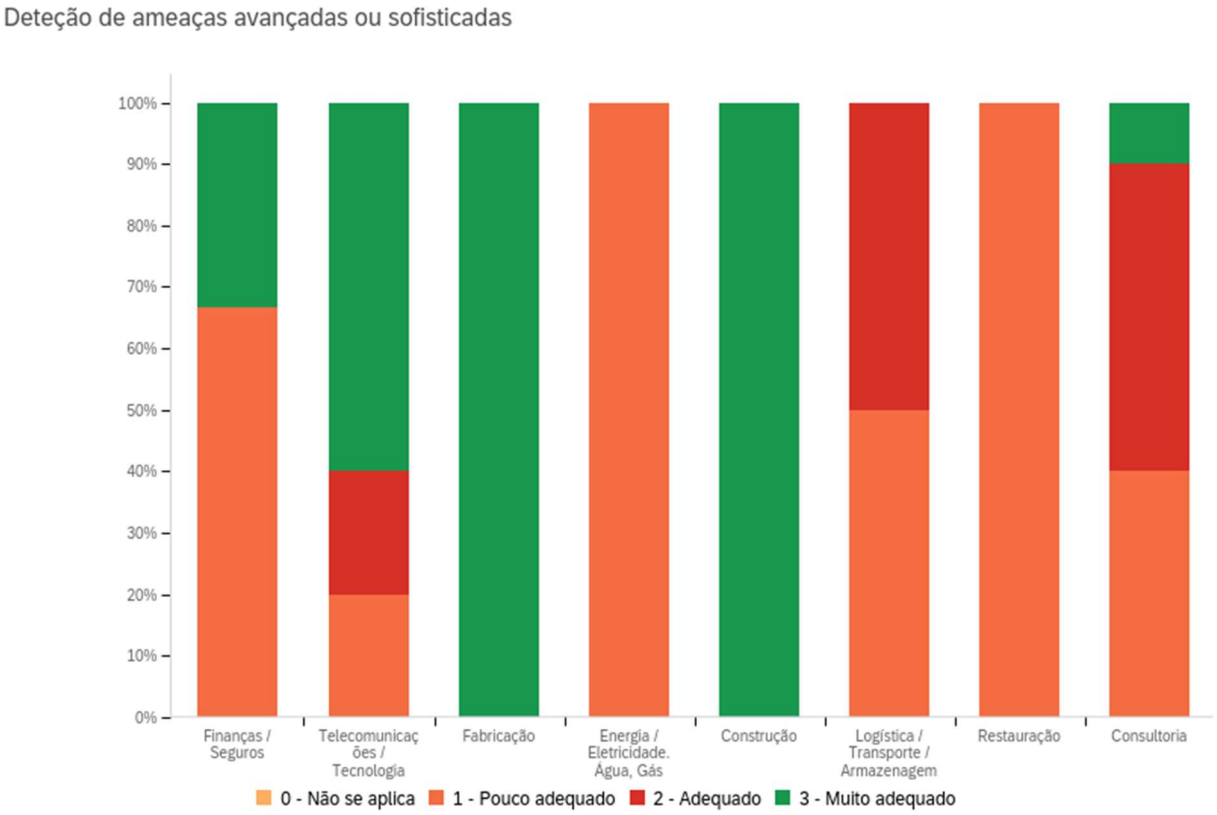

Figura 42: Nível de adequação de deteção de ameaças sofisticadas, por setor de atividade

5.4. Ações das organizações no desenvolvimento da maturidade da Segurança da Informação

Antunes et al. (2021) divide a maturidade de segurança da informação de uma organização em três segmentos: Pessoas, Processos e Tecnologia. No âmbito dos recursos humanos, os participantes foram questionados em quais são as competências de mais-valia para a organização e o nível de robustez do programa de consciencialização dos perigos cibernéticos.

A consciencialização de SI deve ser direcionada para a organização como um todo, no entanto iniciativas que visam um grupo em específico, por exemplo um departamento, podem trazer benefícios que uma iniciativa generalizada não alcança. Abordar assuntos de SI que são relevantes para um determinado departamento da organização cria interesse por parte dos que não são da área tecnológica, com isso os demais colaboradores se tornam parte da defesa cibernética da organização. A Figura 43 representa a perceção dos participantes quanto à robustez do programa de consciencialização da organização, por setor de atividade.

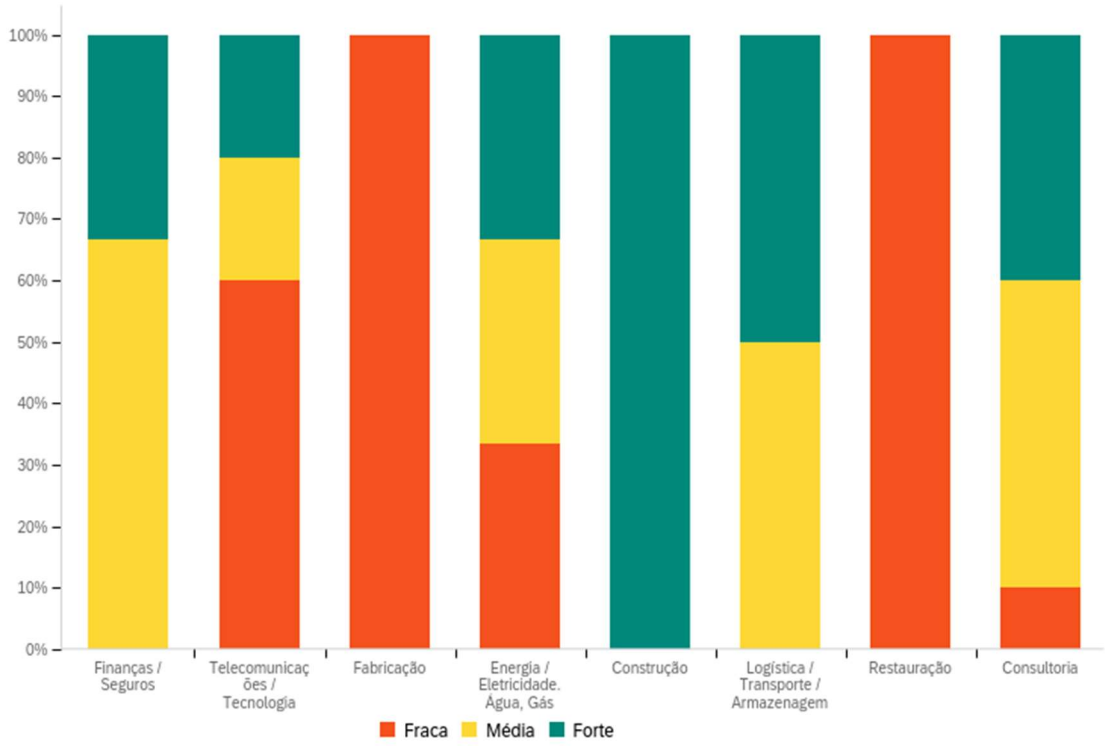

Figura 43: Robustez do programa de consciencialização em SI na organização, por setor de atividade

Uma outra ação extremamente importante para abordar os problemas de SI relacionados às pessoas da própria área são as formações técnicas. Os participantes foram questionados sobre quais são as competências (uma ou mais) de mais-valia para a organização e na Figura

44 está representado que é preciso ter uma ou mais equipas com conhecimentos diversificados. A pluralidade de conhecimentos torna possível, do ponto de vista técnico, a implementação da SI através de diversas iniciativas de forma simultânea e que normalmente precisam de habilidades diferentes, que variam desde configuração técnica de equipamentos, resposta a incidentes e desenvolvimento seguro de software, à consciencialização aos colaboradores e gestão do departamento de SI.

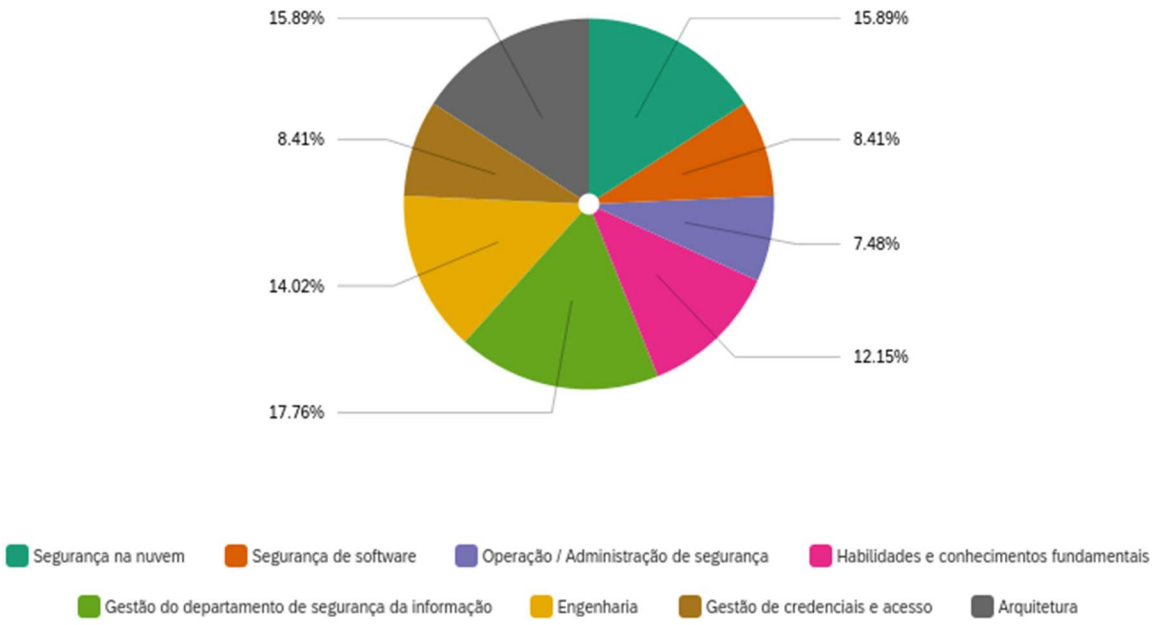

Figura 44: Competências técnicas em SI desejadas pelas organizações (%)

Já no âmbito dos processos, os participantes foram questionados se a organização possui um conjunto de políticas, normas e procedimentos e se são atualizados de forma recorrente. O uso de documentos normativos torna o que é "implicitamente óbvio" do ponto de vista da SI em algo oficialmente definido pela empresa. Especificamente, as políticas servem para a organização demonstrar quais são as diretrizes que toda a corporação deve seguir, assim como as sanções cabíveis em caso de descumprimento, dessa forma fica delineada a estratégia que, por sua vez, serve como principal motivador para a criação de normas e procedimentos que, no caso do primeiro, atuam no mapeamento tático dos diferentes serviços de SI e, do último, na instrução operacional de um determinado serviço.

A Figura 45 representa a utilização de tais documentos normativos para cada setor de atividade dos participantes e é possível identificar que, salvo poucas exceções, há um comportamento padrão entre as organizações de diferentes setores de criar e manter documentos normativos para a área de segurança da informação.

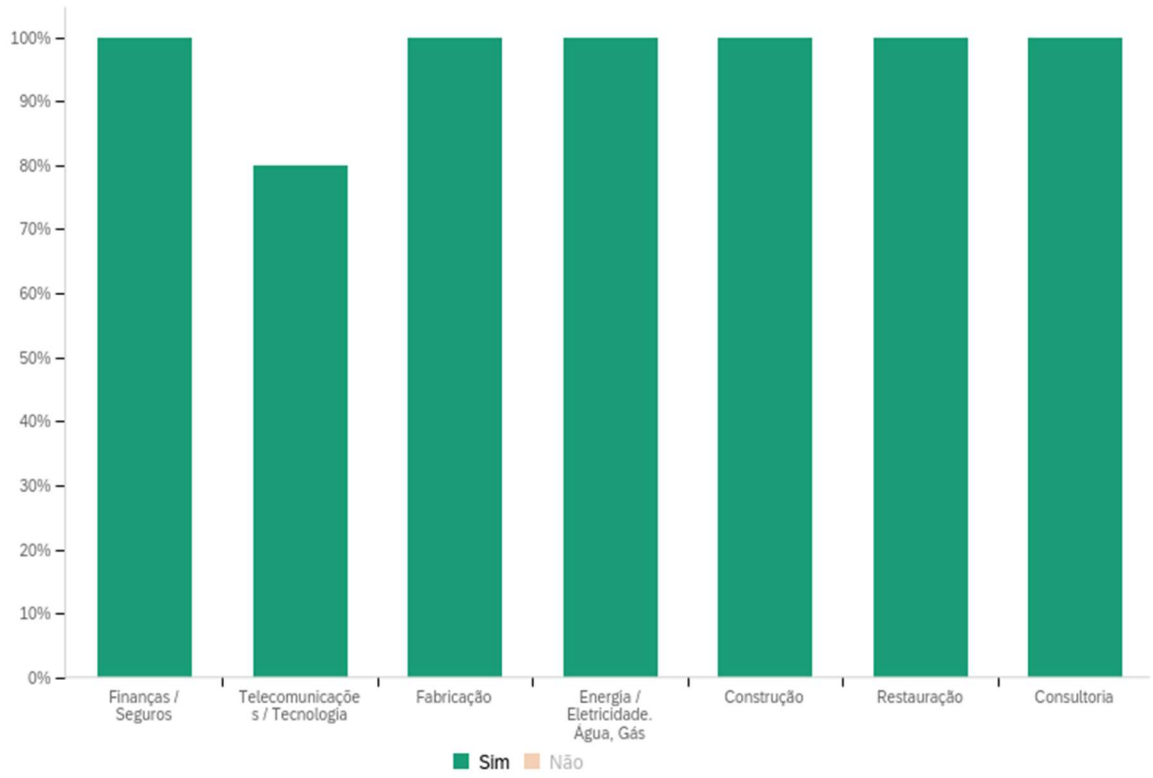

Figura 45: Utilização de documentos normativos, por setor de atividade

Outro ponto relevante para a área de SI é a utilização de frameworks de referência ou padrões reconhecidos internacionalmente e o inquérito tinha como questão se a organização do respondente tinha o padrão ISO/IEC 27001 (*Information security, cybersecurity and privacy protection - Information security management systems – Requirements*) como referência. Este padrão reconhecido internacionalmente foi criado e é atualizado regularmente pela organização ISO (*International Organization for Standardization*) e serve como referência para qualquer empresa de qualquer tamanho e setor de atividade. Apesar de não ser algo obrigatório, pode ser utilizada como fator crítico para o sucesso pois possui um conjunto de requisitos e controlos para guiar a organização num caminho de excelência e maturidade de SI.

Na Figura 46, 54% responderam que seguem a ISO/IEC 27001 como referência. Quando estas respostas são sobrepostas por setor de atividade, fica claro que os setores de Consultoria, Finanças e Seguros, Energia e serviços básicos possuem mais interesse ou familiaridade com este padrão internacional.

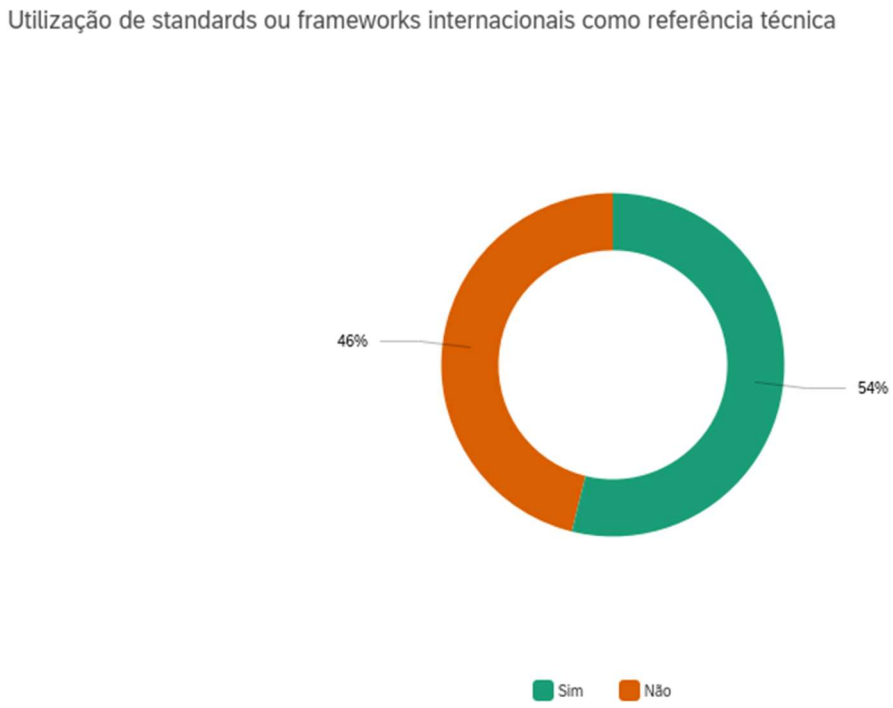

Figura 46: Utilização de standards ou framework internacionais (%)

A Figura 47 representa a distribuição, por setor de atividade, das respostas que afirmam utilizar um standard ou framework como referência técnica.

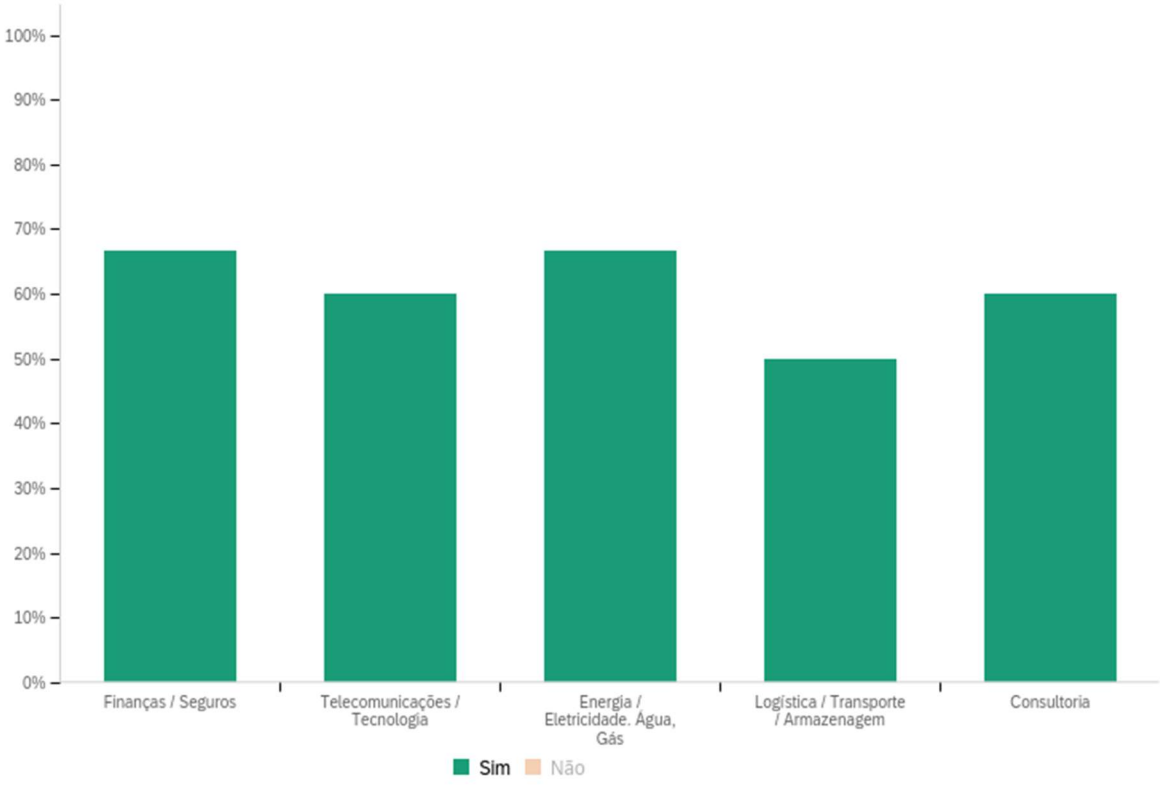

Figura 47: Utilização da ISO/IEC 27001 como referência, por setor de atividade.

No âmbito do terceiro segmento da maturidade de SI, Tecnologias, os respondentes foram questionados sobre a percentagem da infraestrutura da organização que está localizada na nuvem, como por exemplo AWS (Amazon), Azure (Microsoft) e Google Cloud. A Figura 48 representa estas respostas sobrepostas aos setores de atividade.

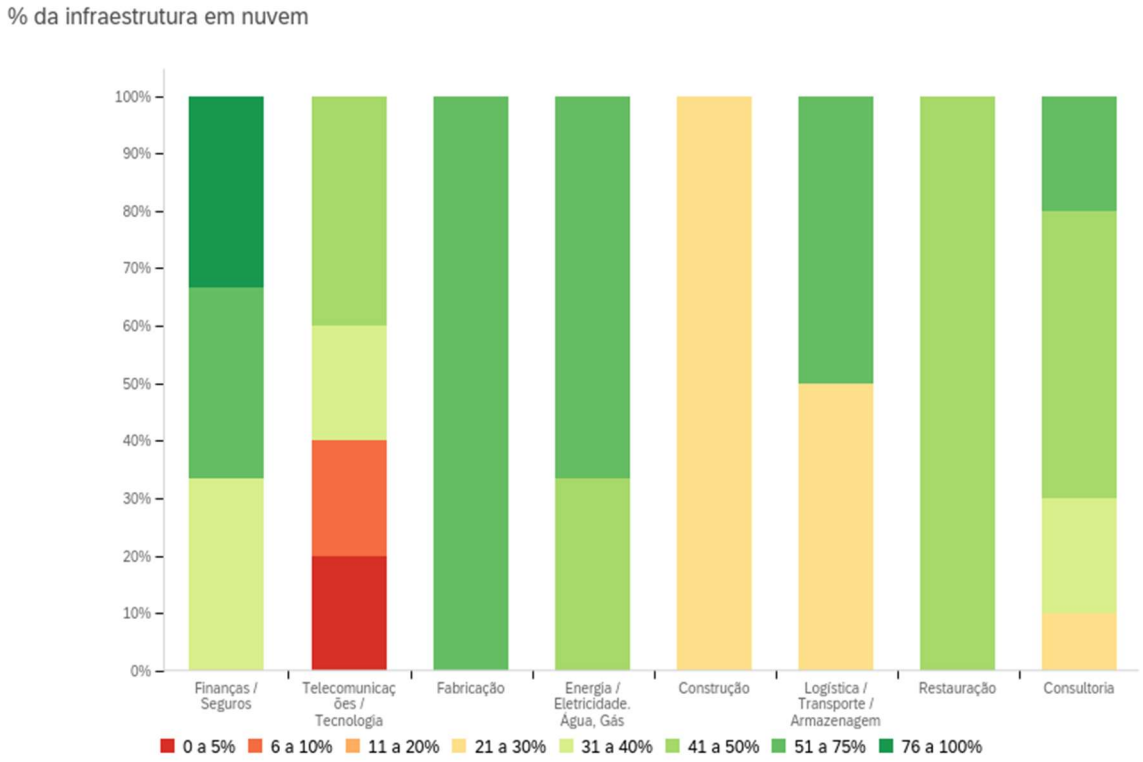

Figura 48: Utilização de infraestrutura em nuvem, por setor de atividade

Uma das grandes diferenças entre infraestrutura em nuvem e *on-premises*, é a redução de custos com a manutenção da mesma. Quando está localizada em nuvem, os custos referentes ao controlo de humidade e temperatura, por exemplo, são terceirizados para o fornecedor (Amazon, Microsoft, Google, entre outros) da infraestrutura em nuvem assim como a obrigatoriedade da disponibilidade, que é 99,999%. Estes dois fatores (disponibilidade e custo) permitem que a organização forneça uma solução ao cliente final de maneira mais segura e abre espaço no orçamento para investimento em outras iniciativas de SI. Essa perceção é representada na Figura 49, onde todos os participantes indicam que sua infraestrutura em nuvem, independente da percentagem, classificam-na como “Segura” ou “Muito Segura”.

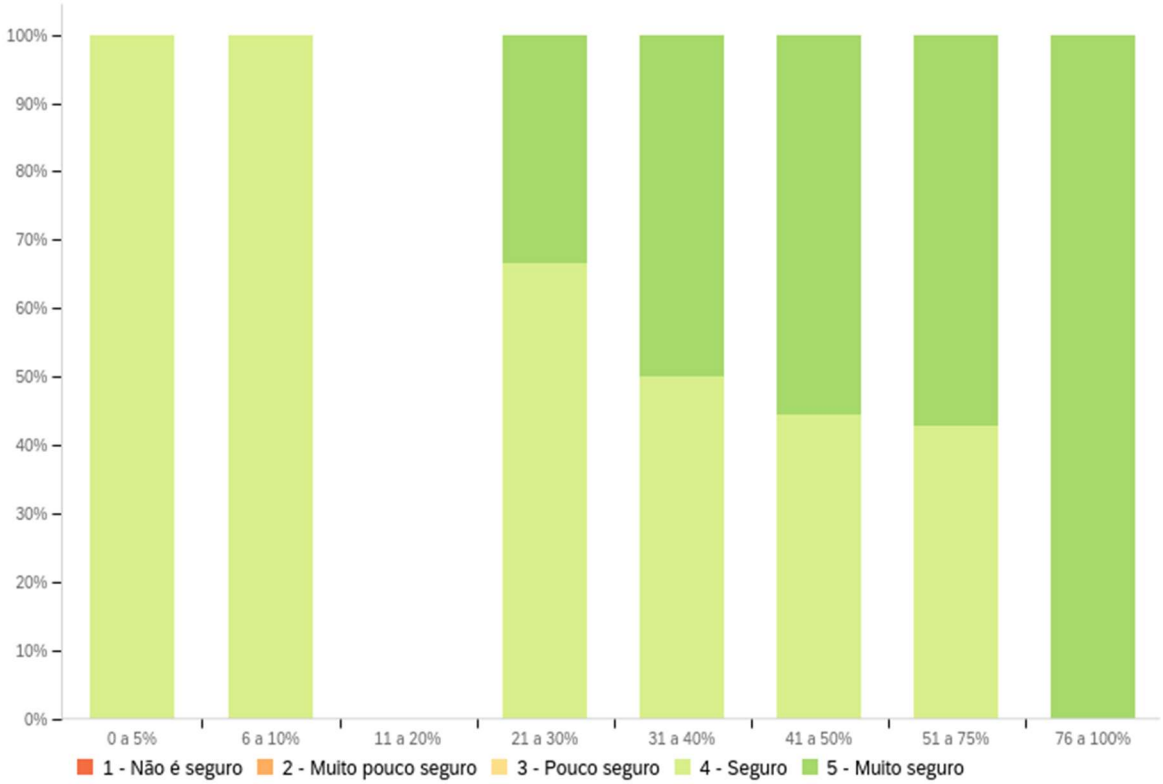

Figura 49: Relação utilização de infraestrutura em nuvem e perceção do nível de segurança

Outro fator tecnológico importante é a proteção de aplicações web e *mobile*, que são expostos ao público para realização de transações financeiras, consultas de informação, entre tantos outros objetivos. Estes aplicativos frequentemente são alvos de ataques cibernéticos por agentes maliciosos, portanto os participantes foram questionados sobre quais são os mecanismos implementados na organização para a devida correção de vulnerabilidades e proteção contra ataques cibernéticos. A Figura 50 mostra a relação entre os mecanismos e a preocupação dos participantes com ataques direcionados a aplicações web e *mobile*.

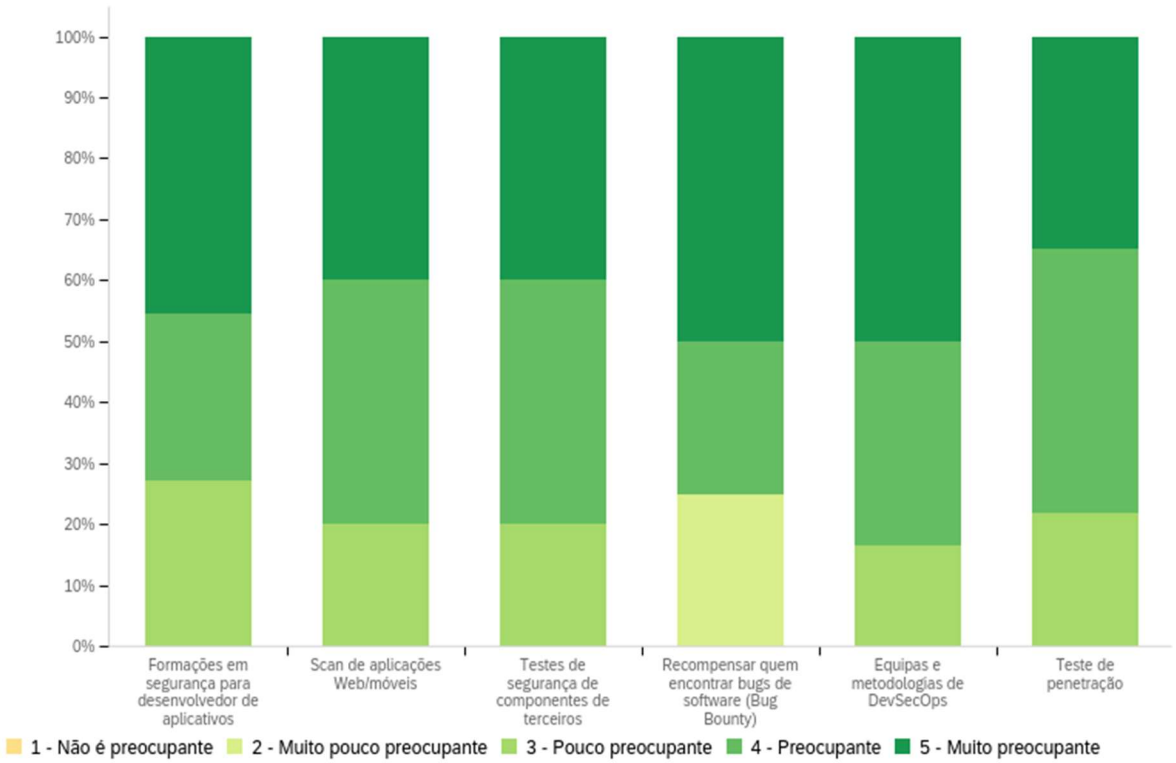

Figura 50: Relação entre os mecanismos de proteção de aplicações web/mobile e preocupação com ataques direcionados a estas aplicações

Uma evolução tecnológica que foi acelerada pela pandemia COVID-19 é o recurso do teletrabalho. O que antes era um recurso, em sua maioria, exclusivo aos profissionais da área de tecnologia devido a natureza da profissão, atualmente é transversal para muitas profissões pelo facto da tecnologia ter evoluído ao ponto de conseguir compreender a carga de trabalho gerada por tantos acessos remotos simultâneos. Com base nisso, a Figura 51 representa as respostas quanto a organização possuir algum mecanismo que possibilite o teletrabalho de forma segura, visto que a empresa não controla a rede de onde o profissional está a se conectar e, em muitos casos, o portátil pessoal é utilizado no lugar de uma estação de trabalho.

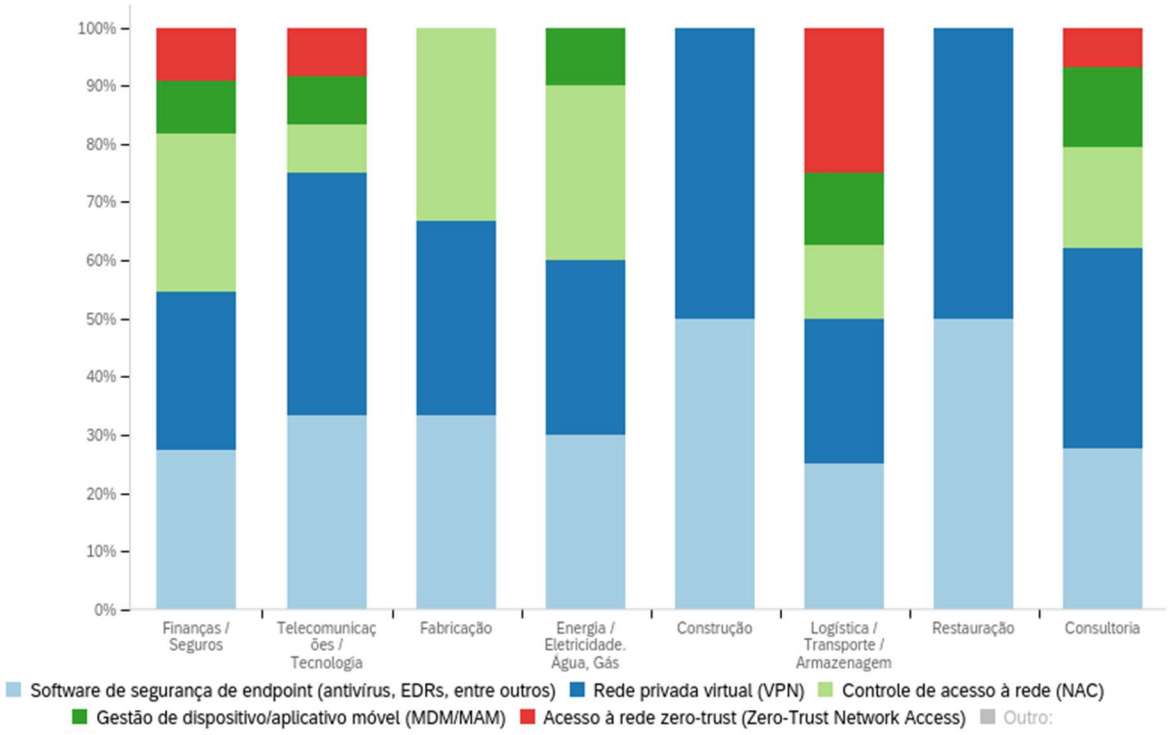

Figura 51: Mecanismos da organização para possibilitar o teletrabalho de forma segura, em percentagem

O apoio da tecnologia, especificamente da SI, ao teletrabalho só é possível devido aos investimentos realizados durante o período da pandemia COVID-19 e é nesse sentido que a Figura 52 representa se o orçamento do ano de 2023 será menor, igual ou maior ao de 2022.

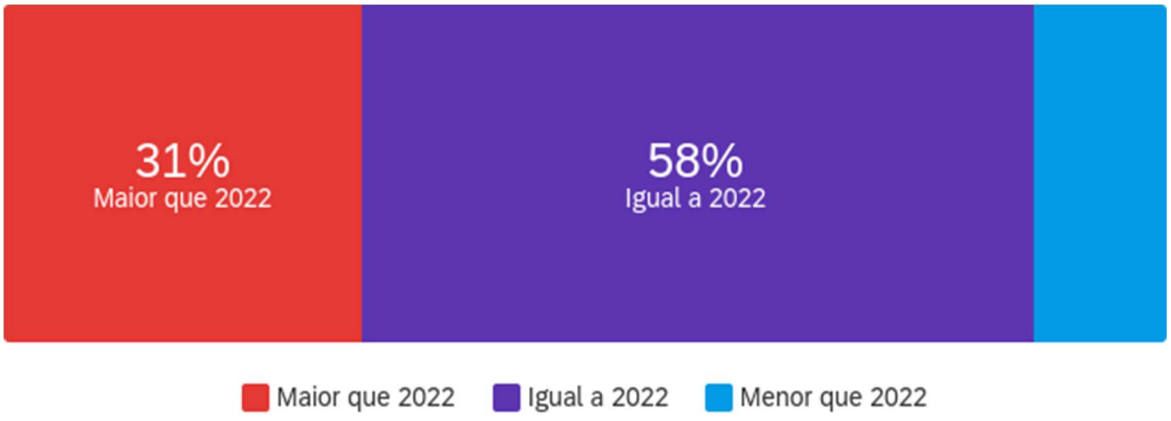

Figura 52: Orçamento de SI de 2023 face ao de 2022

Essa questão é importante pois os valores disponíveis para investimentos em tempos de crise ou outros momentos atípicos são anormalidades no orçamento da área da SI, portanto quando esta questão é sobreposta com a percentagem do orçamento em tecnologia destinada à SI, a relação é representada pela Figura 53, onde é possível identificar que os participantes que possuem orçamento entre 0% e 5% têm a inclinação para manter o orçamento igual ao

de 2022, no entanto, uma vez ultrapassada a barreira dos 5% há uma tendência para aumento do orçamento de 2023 face ao de 2022.

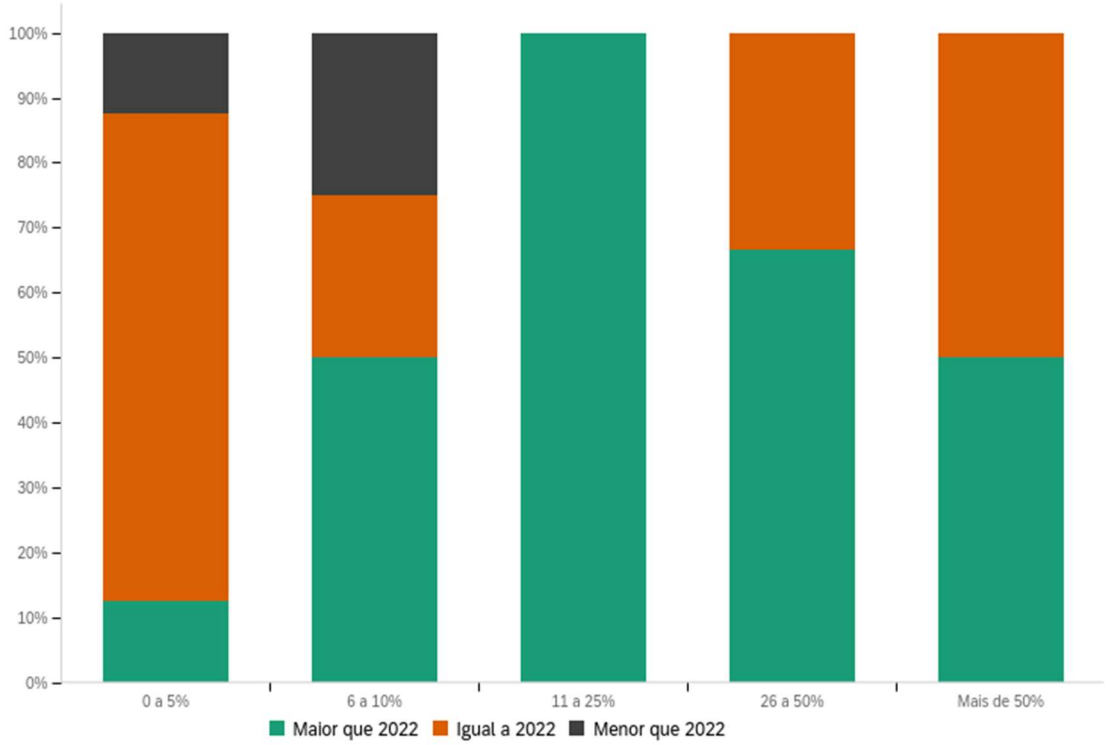

Figura 53: Relação entre orçamentos para SI e evolução de 2022 a 2023

6. Conclusões

O panorama do mundo cibernético tem evoluído numa frequência exponencial e com isso os recursos tecnológicos têm encontrado seu espaço no quotidiano das pessoas. Há alguns anos o conceito de VPN (*Virtual Private Network* – Rede Privada Virtual) era algo inimaginável para algumas pessoas, hoje é algo que qualquer profissional sabe explicar o objetivo e como utilizá-la, mesmo que a pessoa seja de uma área que não é relacionada com tecnologia.

No entanto, os recentes anos não trouxeram apenas vantagens. Os atores mal-intencionados também evoluíram rapidamente e, em alguns casos, até mais rápido do que as capacidades de defesa cibernética. Em 2022, uma mudança importante foi detetada tanto pelo órgão nacional de cibersegurança, CNCS, quanto pela agência europeia responsável por definir diretrizes de cibersegurança para toda a União Europeia, a ENISA, relacionada com o tipo de ameaça número um para a qual as organizações portuguesas e do mundo deveriam, e ainda devem, se preocupar. Essa mudança começou, mais precisamente, no contexto da pandemia COVID-19, onde as preocupações se voltaram para as ameaças que exploram as fraquezas humanas como a engenharia social, nomeadamente o *phishing* para a maioria dos casos, no entanto o que é recomendado pelos órgãos mencionados é o reforço dos controlos de cibersegurança que mitiguem o risco de sequestro de dados, também conhecido como *ransomware*. Este tipo de ataque tornou-se o novo método favorito de malfeitores devido à fragilidade de infraestruturas e, aliado a isso, fatores como a falta de conhecimento dos utilizadores, a utilização de dispositivos pessoais para o teletrabalho, entre tantos outros comportamentos que só surgiram devido a pandemia.

Os ataques de sequestro de dados não ficaram apenas no campo da teoria como pôde ser visto nos últimos anos nos noticiários. Os ataques sofridos por empresas nacionais e internacionais causam grandes danos tanto à empresa quanto ao consumidor e os casos que ocorreram no estrangeiro que valem a pena serem destacados são a Colonial Pipeline, Brenntag, Acer, JBS Foods, Quanta Services e a Kaseya, que somados totalizaram cerca de U$189,8 milhões de dólares requisitados pelo resgate dos dados. Já no mercado doméstico, os destaques são a Germano de Sousa, Vodafone, The Navigator Company, Grupo Imprensa, inclusive hospitais não ficaram livres de ataques, como é o caso dos hospitais Garcia da Orta, o de Ponta Delgada, o de Guimarães, a CUF e outros serviços essenciais como o de transporte, nomeadamente o Serviços Municipalizados de Transportes Urbanos de Coimbra.

No âmbito deste estudo, os vinte e oito respondentes de diversos setores de atividade responderam as diversas questões do inquérito pertinentes à segurança da informação, como as ameaças com as quais mais se preocupam, como está a evoluir o orçamento para a área da segurança da informação, quais tecnologias têm utilizado para a defesa cibernética e

teletrabalho, assim como quais dificuldades têm encontrado em diversas esferas, nomeadamente tecnologia, finanças e recursos humanos, com o intuito de identificar o estado atual das organizações portuguesas no quesito segurança da informação. Este estudo representa uma pequena amostra da realidade das organizações portuguesas, portanto este tema carece de uma pesquisa mais abrangente e que esteja atenta às nuances de cada setor de atividade. Outras linhas de pesquisa relevantes neste tema podem estar mais associadas, por exemplo, com a verificação da eficácia de auditorias face a maturidade em segurança da informação de uma organização, ou o impacto do suporte da gestão de topo na implementação eficaz da segurança da informação.

As conclusões desta amostra indicam que atualmente um dos desafios para as organizações portuguesas é a dificuldade de encontrar e reter profissionais qualificados, tanto na gestão do departamento quanto na engenharia, arquitetura e resposta ao incidente. A solução alternativa é investir na formação técnica contínua aos colaboradores e prestadores de serviço da empresa. É possível identificar também pelas respostas que as organizações têm investido também na consciencialização dos utilizadores quanto aos perigos cibernéticos, para que seja possível diminuir os riscos associados aos comportamentos do utilizador, assim como o nível de exposição da organização. Em termos de tecnologias, a adoção a computação em nuvem tem permitido que as organizações diminuissem o risco de indisponibilidade dos seus serviços, devido a natureza da infraestrutura em nuvem. Aplicações web e *mobile* são as principais superfícies de ataque devido a interação com consumidores externos e as boas práticas da área como testes de penetração, varredura de vulnerabilidades e teste de componentes de software têm ajudado as organizaçoes na diminuição da exposição e do risco à patamares aceitáveis. Além disso, a utilização de *frameworks* e padrões internacionais como ponto de referência para a implementação de maneira estruturada da segurança da informação tem contribuído de maneira significativa para a progressão da maturidade das organizações quanto à sensibilidade desta área, permitindo o planeamento, adequado as limitações financeiras, de curto a longo prazo dos controlos de SI eficazes para o combate às ameaças cibernéticas.

Referências Bibliográficas

Antunes, M., & Maximiano, M., & Gomes, R., & Pinto, D. (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, *1*(2), 219–238. MDPI AG. http://dx.doi.org/10.3390/jcp1020012

Baets, W., & Linden, G. (2003). Virtual Corporate Universities: A Matrix of Knowledge and Learning for the New Digital Dawn (ISIS, volume 2) https://books.google.pt/books?id=2vDlBwAAQBAJ&lpg=PR5&dq=Virtual%20Corporate%20Universities%3A%20A%20Matrix%20of%20Knowledge%20and%20Learning%20for%20the%20New%20Digital%20Dawn&hl=pt-PT&pg=PR5#v=onepage&q&f=false

Burkett, J. (2012). Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA®. *Information Security Journal: A Global Perspective*, *21*(1), 47–54. https://doi.org/10.1080/19393555.2011.629341

Carvalho, J.V., & Carvalho, S. & Rocha, Á. (2020). European strategy and legislation for cybersecurity: implications for Portugal. Cluster Comput 23, 1845–1854. https://doi.org/10.1007/s10586-020-03052-y

Centro Nacional de Cibersegurança. (2021). Relatório Cibersegurança em Portugal – Risco e Conflitos 2021 https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cncs.pdf

Centro Nacional de Cibersegurança (2022). Relatório Cibersegurança em Portugal – Risco e Conflitos 2022, https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf

Centro Nacional de Cibersegurança. (2022). Relatório Cibersegurança em Portugal – Economia 2022. https://www.cncs.gov.pt/docs/relatorio-economia2022-obciber-cncs.pdf

Centro Nacional de Cibersegurança. (2022). Contexto atual da cibersegurança no país. https://www.cncs.gov.pt/pt/contexto-atual/

Chapple, M., & Stewart, J. M., & Gibson, D. (ISC)² CISSP Certified Information Systems Security Professional Official Study Guide (2018). https://books.google.pt/books?id=psJVDwAAQBAJ&lpg=PR33&ots=j3TM4yDRW3&dq=cissp%20official%20study%20guide%20%202021%20mike%20chapple&lr&hl=pt-PT&pg=PR33#v=onepage&q&f=false

Collier, Z. A. & Sarkis, J. (2021) The zero trust supply chain: Managing supply chain risk in the absence of trust, International Journal of Production Research. https://doi.org/10.1080/00207543.2021.1884311

Corallo, A., Lazoi, M., Lezzi, M., Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. https://doi.org/10.1016/j.compind.2022.103614

Cuganesan, S., & Steele, C., & Hart, A. (2018) How senior management and workplace norms influence information security attitudes and self-efficacy, behaviour & information technology. https://doi.org/10.1080/0144929X.2017.1397193

CyberEdge Group, 2022 Cyberthreat Defense Report (2022) https://www.isc2.org/-/media/ISC2/Research/Cyberthreat-Defense-Report/2021/CyberEdge-2021-CDR-Report-v10--ISC2-Edition.ashx?la=en&hash=60BC7C7969857E2FF07B714896F079EF5C9C1C39

Desbonnet, J. (2022). Why it's time for a zero-trust conversation, Capgemini Research Institute https://www.capgemini.com/insights/research-library/why-its-time-for-a-zero-trust-conversation/

ENISA – Threat Landscape 2021
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) https://eur-lex.europa.eu/eli/dir/2022/2555

EU GDPR – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) https://eur-lex.europa.eu/eli/reg/2016/679

Federal Trade Comission (FTC) of U.S. Federal Government. (n.d.). Privacy Shield: Update on the Privacy Shield Framework https://www.ftc.gov/business-guidance/privacy-security/privacy-shield

Gabinete de Estratégia e Estudos do Ministério da Economia de Portugal. (2018). Estudos de Temas Económicos (TE56 - A Cibersegurança em Portugal)
https://www.gee.gov.pt/pt/estudos-e-seminarios/estudos-de-temas-economicos-category/34-temas-economicos/17741-a-ciberseguranca-em-portugal

Gabinete de Estratégia e Estudos do Ministério da Economia de Portugal. (2018). Estudos de Temas Económicos (TE54 - A Economia da Cibersegurança) https://www.gee.gov.pt/pt/estudos-e-seminarios/estudos-de-temas-economicos-category/17739-a-economia-da-ciberseguranca

Gordon, L., & Loeb, M., & Sohail, T. (2003). A Framework for Using Insurance for Cyber-Risk Management. Communications of the ACM, March 2003, Vol. 46, No. 3.
https://cacm.acm.org/magazines/2003/3/6869-a-framework-for-using-insurance-for-cyber-risk-management/fulltext

Istikoma, & Fakhri, N., & Qurat-al-Ain, & Jamaludin, I. (2015). Information Security Aligned to Enterprise Management. (2015). *Middle East Journal of Business*, *10*(1), 62. https://doi.org/10.5742/MEJB.2015.92601

NATO: For Your Eyes Only - What is security classification? https://www.nato.int/cps/en/natohq/declassified_138449.htm

NIST Computer Security Research Center. (2022). Definição de Segurança da Informação. https://csrc.nist.gov/glossary/term/information_security

NIST. (2022). NIST Cybersecurity Framework. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Kaspersky Labs. (n.d.). The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. https://www.kaspersky.com/blog/the-human-factor-in-it-security/

SANS Institute. (2012). People, Process, and Technologies Impact on Information Data Loss. https://www.sans.org/reading-room/whitepapers/dlp/people-process-technologies-impactinformation-data-loss-34032

Anexos

Anexo A – Inquérito "A realidade da cibersegurança nas organizações portuguesas"

A realidade da cibersegurança nas organizações portuguesas

Start of Block: Default Question Block

Secção 1 O presente questionário visa identificar as preocupações das organizações portuguesas na matéria Segurança da Informação, bem como as consequências da falta dela, num contexto de evolução acelerada pela pandemia.

As respostas a este questionário são anónimas e confidenciais. A resposta a este questionário demora cerca de 7 minutos. Por favor, reserve o tempo necessário para responder a todas as questões.

A sua opinião é muito importante para nós, pelo que pedimos que responda com o máximo de rigor e honestidade.

Número de trabalhadores na organização

- ○ 1 - 10 (1)
- ○ 11 – 49 (2)
- ○ 50 – 99 (4)
- ○ 100 – 249 (5)
- ○ 250 - 499 (6)
- ○ 500 – 999 (7)
- ○ 1,000 – 4,999 (8)
- ○ Mais de 5,000 (9)

Secção 1 Setor de atividade da organização

▼ Finanças / Seguros (1) ... Consultoria (13)

Secção 1 Localização da organização

- ○ Sede em Portugal (1)
- ○ Apenas sucursais em Portugal (2)

Page Break

Secção 2 Indique o grau de preocupação da sua organização com cada uma das seguintes ameaças cibernéticas.

Malware (vírus, worms, Trojans) (1)	▼ 1 - Não é preocupante (16) ... 5 - Muito preocupante (20)
Ataques de invasão de conta/abuso de credenciais (2)	▼ 1 - Não é preocupante (16) ... 5 - Muito preocupante (20)
Ransomware (3)	▼ 1 - Não é preocupante (16) ... 5 - Muito preocupante (20)
Ataques de Phishing / spear-phishing (4)	▼ 1 - Não é preocupante (16) ... 5 - Muito preocupante (20)
Ataques à marca e reputação nas redes sociais e na web (5)	▼ 1 - Não é preocupante (16) ... 5 - Muito preocupante (20)
Ameaças persistentes avançadas (APTs) (6)	▼ 1 - Não é preocupante (16) ... 5 - Muito preocupante (20)
Ataques de Negação de Serviço (DoS/DDoS) (7)	▼ 1 - Não é preocupante (16) ... 5 - Muito preocupante (20)
Ataques a aplicações web (8)	▼ 1 - Não é preocupante (16) ... 5 - Muito preocupante (20)
Ameaças internas / vazamento de dados por colaboradores (9)	▼ 1 - Não é preocupante (16) ... 5 - Muito preocupante (20)
Ataques zero-day (vulnerabilidades desconhecidas) (10)	▼ 1 - Não é preocupante (16) ... 5 - Muito preocupante (20)

Page Break

Secção 2 Indique como os aspetos seguintes podem impactar a sua organização na defesa contra ameaças cibernéticas.

Falta de profissionais qualificados (1)	▼ 1 - Muito baixo impacto (17) ... 5 - Muito alto impacto (21)
Baixa consciencialização de segurança da informação entre os colaboradores (internos e prestadores de serviço) (2)	▼ 1 - Muito baixo impacto (17) ... 5 - Muito alto impacto (21)
Fraca integração/interoperabilidade entre soluções de segurança (3)	▼ 1 - Muito baixo impacto (17) ... 5 - Muito alto impacto (21)
Falta de suporte/conscientização da gestão (4)	▼ 1 - Muito baixo impacto (17) ... 5 - Muito alto impacto (21)
Muitos dados para analisar (5)	▼ 1 - Muito baixo impacto (17) ... 5 - Muito alto impacto (21)

Secção 3 Indique o nível de segurança da informação da sua organização (capacidade de se defender contra ameaças cibernéticas) em cada um dos seguintes componentes:

Endpoints (desktops, portáteis, telemóveis, entre outros) (1)	▼ 1 - Não é seguro (16) ... 5 - Muito seguro (20)
Websites/aplicações da web e contêineres (2)	▼ 1 - Não é seguro (16) ... 5 - Muito seguro (20)
Infraestrutura e aplicações em nuvem (SaaS, PaaS, IaaS) (3)	▼ 1 - Não é seguro (16) ... 5 - Muito seguro (20)
Infraestrutura on-premises (servidores, redes, banco de dados, entre outros) (4)	▼ 1 - Não é seguro (16) ... 5 - Muito seguro (20)
Interfaces de programas de aplicativos (APIs) (5)	▼ 1 - Não é seguro (16) ... 5 - Muito seguro (20)

Secção 2 Indique se a sua organização foi alvo de sequestro de dados (ransomware) nos últimos 12 meses.

- ○ Sim e foi pago o resgate (1)
- ○ Sim, mas não foi pago o resgate (2)
- ○ Não (4)
- ○ Prefiro não responder (5)

Secção 3 Indique o número de vezes que um ataque cibernético, direcionado à sua organização, foi bem-sucedido nos últimos 12 meses.

- ○ Nenhuma vez (1)
- ○ Entre 1 a 5 vezes (2)
- ○ Entre 6 a 10 vezes (3)
- ○ Mais de 10 vezes (4)

Secção 3 Avalie a probabilidade de um ataque cibernético, direcionado à sua organização, ser bem-sucedido nos próximos 12 meses.

- ○ Muito baixa (1)
- ○ Baixa (2)
- ○ Possível (3)
- ○ Alta (4)
- ○ Muito alta (5)

Page Break

Secção 3 Avalie a postura das suas áreas da segurança da informação face aos requisitos da sua organização.

Governança, risco e conformidade (GRC) (12)	▼ 0 - Não se aplica (6) ... 3 - Muito adequado (9)
Gestão de identidade e acesso (IAM) (13)	▼ 0 - Não se aplica (6) ... 3 - Muito adequado (9)
Deteção de ameaças avançadas/sofisticadas (14)	▼ 0 - Não se aplica (6) ... 3 - Muito adequado (9)
Desenvolvimento seguro (SSDLC) (15)	▼ 0 - Não se aplica (6) ... 3 - Muito adequado (9)
DevSecOps (16)	▼ 0 - Não se aplica (6) ... 3 - Muito adequado (9)
Investigação e resposta a incidentes (17)	▼ 0 - Não se aplica (6) ... 3 - Muito adequado (9)
Redução da superfície de ataque (18)	▼ 0 - Não se aplica (6) ... 3 - Muito adequado (9)

Secção 2 Indique a percentagem do orçamento em tecnologia que é alocada para segurança da informação (Pessoas, Processos e Tecnologia).

- ○ 0 a 5% (9)
- ○ 6 a 10% (10)
- ○ 11 a 25% (11)
- ○ 26 a 50% (12)
- ○ Mais de 50% (13)

Secção 4 Compare o orçamento para segurança da informação da sua organização em 2023 face a 2022.

- ○ Maior que 2022 (1)
- ○ Igual a 2022 (2)
- ○ Menor que 2022 (3)

Secção 4 Indique a percentagem de aplicativos e serviços de segurança da informação da organização que são entregues por cloud service providers (e.g. AWS, Azure, Google, etc.).

- ○ 0 a 5% (1)
- ○ 6 a 10% (2)
- ○ 11 a 20% (3)
- ○ 21 a 30% (4)
- ○ 31 a 40% (5)
- ○ 41 a 50% (6)
- ○ 51 a 75% (7)
- ○ 76 a 100% (8)

Secção 2 Indique quais os ataques direcionados a aplicações web e aplicativos mobile que são mais preocupantes para a sua organização.

- [ ] Recolha de dados pessoais indevida (1)
- [ ] Ataques de invasão de conta / Roubo de credenciais (2)
- [ ] Fraude ou ataques de cartão/pagamento (3)
- [ ] Ataques de negação de inventário (4)
- [ ] Outro. Qual? (5) _____

Secção 4 Indique quais as práticas que a sua organização adota para aprimorar a segurança de aplicativos/aplicações web (Selecione todas as opções que se aplicam).

- [ ] Formações em segurança para desenvolvedor de aplicativos (1)
- [ ] Scan de aplicações Web/móveis (2)
- [ ] Testes de segurança de componentes de terceiros (3)
- [ ] Recompensar quem encontrar bugs de software (Bug Bounty) (4)
- [ ] Equipas e metodologias de DevSecOps (5)
- [ ] Teste de penetração (6)

Page Break

Secção 3 Selecione as funções/áreas para as quais a sua organização está a enfrentar dificuldades para encontrar profissionais de segurança da informação (SI) qualificados. (Selecione todas as opções que se aplicam).

- [ ] Administrador/Analista/Consultor de SI (1)
- [ ] Gestor de SI (2)
- [ ] Arquiteto/engenheiro de SI (3)
- [ ] Auditor de segurança/conformidade de SI (4)
- [ ] Diretor de SI (5)
- [ ] Analista de risco/fraude cibernético (6)
- [ ] Operador/respondedor de incidentes (7)
- [ ] Analista/testador de segurança de aplicações móveis/web (8)
- [ ] DevSecOps (9)
- [ ] Outro: (10) _____

Secção 4 Indique quais as áreas de certificação de competências em segurança cibernética que trazem mais valor para a sua organização.

- [ ] Segurança na nuvem (1)
- [ ] Segurança de software (2)
- [ ] Operação / Administração de segurança (3)
- [ ] Habilidades e conhecimentos fundamentais (4)
- [ ] Gestão do departamento de segurança da informação (5)
- [ ] Engenharia (6)
- [ ] Gestão de credenciais e acesso (7)
- [ ] Arquitetura (8)

Secção 4 Indique quais as tecnologias e/ou arquiteturas que a sua organização utiliza para permitir que os funcionários realizem teletrabalho com segurança.
(Selecione todas as opções que se aplicam)

- [ ] Software de segurança de endpoint (antivírus, EDRs, entre outros) (1)
- [ ] Rede privada virtual (VPN) (2)
- [ ] Controle de acesso à rede (NAC) (3)
- [ ] Gestão de dispositivo/aplicativo móvel (MDM/MAM) (4)
- [ ] Acesso à rede zero-trust (Zero-Trust Network Access) (5)
- [ ] Outro: (6) _____

Secção 4 Indique a robustez das iniciativas de consciencialização de segurança direcionada ao teletrabalho na sua organização.

- ○ Fraca (1)
- ○ Média (2)
- ○ Forte (3)

Secção 3 Indique se sua organização possui um conjunto de Políticas e Processos de segurança da informação atualizados regularmente.

- ○ Sim (1)
- ○ Não (2)

Secção 4 Indique se já implementou ou está a implementar um SGSI (Sistema de Gestão de Segurança da Informação) na sua organização, usando como referência a ISO/IEC 27001.

- ○ Sim (1)
- ○ Não (2)

End of Block: Default Question Block