INSTITUTO SUPERIOR
DE TECNOLOGIAS
AVANÇADAS DE LISBOA

Segurança e Integridade da Informação em contexto organizacional

Ayrton Décio de Jesus Jorge

Dissertação para obtenção do Grau de Mestre em

INFORMÁTICA

Júri

Presidente: Prof. Doutor Paulo André Reis Duarte Branco

Orientador: Prof. Doutor Pedro Ramos dos Santos Brandão

Arguente: Professor Doutor Pedro Manuel Ferreira Raposo Torres Brás

Outubro, 2021

Aos meus Pais pelo amor e apoio incondicional.
À minha irmã Joelma por todo o seu incentivo.
À minha esposa Alexandra pela sua compreensão
em todos os momentos de estudo e reflexão.
À minha filha Isabela para que a dedicação ao conhecimento,
seja sempre uma constante na sua vida.
Ao meu primo David pela sua excelente amizade.

Agradecimentos

A conclusão deste trabalho é um momento de alegria, mas igualmente um momento para agradecer a todos que contribuíram para que fosse possível a sua concretização.

Em primeiro lugar, quero agradecer ao Professor Doutor Pedro Brandão, meu orientador, pela partilha de conhecimento, e pela aprendizagem que me proporcionou, através de críticas construtivas e sugestões de melhoria.

Agradecer ao Professor Doutor Paulo Duarte por todas as suas recomendações úteis e pertinentes nas aulas do Seminário.

Agradecer aos colegas deste ciclo de estudos pela partilha de conhecimento e troca de experiências.

Agradecer a todos elementos da equipa administrativa do ISTEC pela sua pronta disponibilidade e serviço de excelência.

Agradecer a todos que se disponibilizaram para participar e difundir o questionário.

Agradecer minha família e em especial à minha mãe Elvira Bondo e minha irmã Joelma Bondo por todo apoio incondicional e suporte neste processo.

A todos o meu profundo agradecimento.

Resumo

Tendo como premissa que a segurança e integridade da informação são questões cruciais em contexto organizacional, e que diariamente representam um dos maiores desafios que o mundo empresarial tem de enfrentar, o presente trabalho tem como propósito o desenvolvimento de uma *framework* de análise das vulnerabilidades de um sistema de informação, com o objectivo de identificar potenciais ameaças e mitigar riscos. Viver num mundo em rede possibilitou um crescimento da capacidade de comunicação de dados, abrindo as portas para serviços e tecnologias comunicação, mineração e armazenamento inimagináveis, o que aumentou também os riscos a que a informação está exposta, podendo mesmo no caso de cair em mãos erradas, ficar indisponível, ser corrompida, ou representar uma ameaça em termos individuais e colectivos. Esta constatação que cruza a história da humanidade, obriga numa era dita de informação a conciliar a protecção em termos técnicos dos próprios sistemas, com os processos e com a segurança ao nível do comportamento das pessoas. Assim, em relação à segurança da informação é elementar que pessoas e organizações entendam que o factor humano consubstancia um dos maiores riscos, dado que a maioria das violações e fugas de informação dos sistemas bem concebidos em termos de segurança são realizadas por pessoas, seja de forma intencional ou acidental. Neste sentido, entende-se que o conjunto de ameaças e vulnerabilidades é dinâmico e altera-se mais rapidamente do que os controles de mitigação, o que impõe a necessidade de investir no desenvolvimento de medidas preventivas, detectivas e correctivas. Por conseguinte, a *framework* desenvolvida, tem como finalidade ser um instrumento de gestão que permita apoiar as organizações numa óptica de antecipação e prevenção. Consiste numa ferramenta prática e ágil que possibilita a quem não pretende implementar um processo de certificação, dispor de um instrumento de recolha da informação necessária para melhor identificar vulnerabilidades e criar as medidas adequadas para dotar a empresa de capacidade de monitorização de riscos.

Palavras-chave: Integridade, Informação, Dados, Vulnerabilidades, Risco, Ameaça

Abstract

On the premises that information security and integrity are crucial issues in the organizational context and that daily they represent one of the greatest challenges that the business world has to face, the purpose of this work is to develop a framework for analysing the vulnerabilities of an information system, to identify potential threats and mitigate risks. Living in a networked world has enabled a growth in data communication capabilities, which opens the door to unimaginable communication, mining, storage services and technologies. This has also increased the risks to which information is exposed, and even if it falls into the wrong hands, it can become unavailable, corrupted, or represent a threat in individual and collective terms. This observation, which crosses the history of humanity, forces us in a so-called information age to reconcile protection in technical terms of the systems themselves, with processes and with security at the level of people's behaviour. Thus, in relation to information security, it is elementary that people and organizations understand that the human factor is one of the biggest risks since most violations and information leaks from well-designed systems in terms of security are carried out by people, either intentionally or accidentally. In this sense, it is understood that the set of threats and vulnerabilities is dynamic and changes faster than the mitigation controls, which imposes the need to invest in the development of preventive, detection, and corrective measures. Therefore, the framework developed aims to be a management tool that allows supporting organizations in an anticipation and prevention perspective. It consists of a practical and agile tool that enables those who do not intend to implement a certification process to have an instrument for collecting the necessary information to identify vulnerabilities better and create the appropriate measures to provide the company with the capacity to monitor risks.

Keywords: Integrity, Information, Data, Vulnerabilities, Risk, Threat

Índice Geral

Índice de Figuras

Índice de Gráficos

Índice de Quadros

Índice de Tabelas

Lista de Abreviaturas

IEC - The International Electrotechnical Commission

ISO - International Standard Organization

LAN – Local Area Network

NIST - National Institute of Standards and Technology

Lista de Siglas

CNSS - Committee on National Security Systems

DLP - Data Lost Protection

IIA - Institute of Internal Auditors, Inc.

IIC’s - Excellence in Information Integrity Award

IoE - Internet of Everything

IS - Information System

ISACA - Information Systems Audit and Control Association

PaaS - Platform as a Service

SaaS - Software as a Service

SGBD - Sistema de Gestão de Base de Dados

SGSI - Sistema de Gestão de Segurança da Informação

SI – Sistema de Informação

SIEM - Security Information Event management

SOAR - Security Orchestration Automated response

TI – Tecnologia de Informação

PARTE I – Teórica

Capítulo 1 - Introdução

A segurança e integridade da informação sempre foram aspectos cruciais em contexto organizacional, realidade que com a digitalização e a *Internet of Everything* (IoE) transformou-se num dos maiores desafios que o mundo empresarial passou a enfrentar. Com bilhões de dispositivos ligados mundialmente, a segurança da informação, deixou de poder ser considerada apenas numa perspectiva técnica, transformando-se num recurso que necessita de ser gerido de maneira adequada e sistemática (Bapty *et al.*,2017; Boeckl *et al.* 2021; Whitman & Mattord, 2017). No entanto, e tendo em consideração as diferenças entre a informação e os outros recursos, assegurar a sua protecção é um processo complexo e multifactorial que obriga ao desenvolvimento de uma cultura de Tecnologia de Informação (TI) segura, alicerçada em tecnologia, mas igualmente em comportamentos, conhecimento e formação (Brandão e Rezende, 2020). Por conseguinte, a segurança da informação não é apenas um problema técnico, mas também um problema de "pessoas", dado que independentemente do número de controles técnicos, a tecnologia por si só, pode não ser suficiente para manter uma organização protegida (Safianu, Twum, & Hayfron-Acquah, 2016).

Efectivamente, viver num mundo em rede permitiu um crescimento sem precedentes da capacidade de comunicação de dados, abrindo as portas para serviços e tecnologias de mineração e armazenamento, até agora inimagináveis, o que, se por um lado traz consigo inúmeras vantagens, por outro, aumentou consideravelmente os riscos a que a informação está exposta, podendo mesmo no caso de cair em mãos erradas, ficar indisponível, ser corrompida, ou representar uma ameaça em termos individuais e colectivos (Alhalafi & Veeraraghavan, 2019; Orvalho, Figueiredo & Pinto, 2020; The IIA, 2019). Neste sentido, a segurança da informação, transformou-se num desafio crescente, que obriga a conciliar a protecção em termos técnicos do próprio sistema, com os processos e com a segurança ao nível do comportamento das pessoas (Ward & Peppard, 2002). Assim, em relação à segurança da informação é fundamental que pessoas e organizações entendam que o factor humano consubstancia um dos maiores riscos, dado que a maioria das violações dos sistemas e fugas de informação são efectuadas por pessoas, seja de forma intencional, seja por negligência (Safianu *et al*., 2016).

Cientes desta realidade e que apesar de existirem outras opções, uma das maneiras mais eficazes de implementar procedimentos de segurança é a implementação de um Sistema de Gestão de Segurança da Informação (SGSI) suportado em normas da família ISO/IEC 27000, mas que também, consiste num sistema complexo, lento e dispendioso (Susanto & Almunawar, 2018), o

presente estudo tem como propósito o desenvolvimento de uma *framework* de análise das vulnerabilidades de um sistema de informação, com o objectivo de identificar potenciais ameaças e mitigar riscos.

Como contributo e resultados esperados, e em sintonia com as orientações *The Institute of Internal Auditors, Inc*., (The IIA, 2016) entende-se que o conjunto de ameaças e vulnerabilidades é dinâmico e altera-se mais rapidamente do que os controles de mitigação, o que impõe a necessidade de investir no desenvolvimento de medidas preventivas, detectivas e correctivas. Por conseguinte, a *framework* a desenvolver, tem como finalidade ser um instrumento de gestão que permita apoiar as organizações numa óptica de antecipação e prevenção.

Neste sentido, pretende-se obter uma ferramenta prática e ágil que possibilite a quem não pretende implementar um processo de certificação, dispor de um instrumento de recolha da informação necessária para melhor identificar vulnerabilidades e criar as medidas adequadas para dotar a empresa de capacidade de monitorização de riscos.

Cumpre salientar que, em contexto organizacional, a segurança da informação é um dos factores essenciais de sucesso e a integridade representa uma questão crucial para sustentar qualquer tomada de decisão, o que atesta a relevância do presente trabalho. Como as ameaças podem ter origem interna e/ ou externas, técnica ou de comportamento humano foi considerado como objectivo - conhecer o tipo de informação interna e externa mais valorizado e utilizado pelas organizações, quais as tecnologias e procedimentos de protecção incorporados e quais os principais constrangimentos por elas já identificados tendo-se definido como questões de investigação analisar se a informação recolhida pelas organizações está devidamente protegida e com que procedimentos? Se a informação armazenada está protegida e salvaguardada a sua integridade? Como são geridos os acessos da informação recolhida e armazenada pelas organizações? E se as novas tecnologias de armazenamento e processamento são uma ferramenta cada vez mais utilizada pelas organizações?

Identificadas as linhas mestras da dissertação é altura de olhar mais pormenorizadamente para a sua estrutura, a qual é composta por duas partes e organizada em seis capítulos.

Na primeira parte apresenta-se a fundamentação teórica e na segunda parte o trabalho prático, como seguidamente se descreve.

Na Parte I, no primeiro capítulo, dado o seu carácter introdutório, apresenta-se a problemática em estudo, os objectivos, as questões de investigação e os resultados esperados com

o desenvolvimento da *framework*. No segundo capítulo, com base na revisão bibliográfica, aborda-se a problemática do papel da informação e dos sistemas em contexto organizacional, salientando os princípios de segurança da informação e a importância da integridade. São ainda apresentadas as principais vulnerabilidades e caracterizadas as ameaças. Por último, mas não menos importante, cruza-se a importância da informação na tomada de decisão, e salienta-se a relevância de gerir o risco.

Na Parte II, no terceiro capítulo, apresenta-se a metodologia, através da descrição das opções metodológicas, dos objectivos e questões de investigação. Descrevem-se os procedimentos efectuados na elaboração dos instrumentos de recolha da informação e os critérios para a construção da amostra. No quarto capítulo, procede-se à apresentação e interpretação dos resultados. No quinto capítulo apresenta-se a *Framework* de análise das vulnerabilidades e no sexto as conclusões e recomendações.

Capítulo 2 – Estado da Arte

2.1 O papel da informação e dos sistemas em contexto organizacional

Ao longo dos anos, o Homem sempre desenvolveu diferentes tipos de estratégias de comunicação e de gestão da informação, seja em contexto militar, político, social ou empresarial. Neste sentido, e independentemente do formato, a informação sempre foi um activo cujo valor difere em função da sua utilidade e pertinência (Whitman & Mattord, 2017). Esta inexistência de homogeneidade de valor é crucial para que a informação seja considerada como um recurso que necessita de ser gerido.

Como explica Rascão (2008) a mesma informação pode assumir valores diferentes para utilizadores distintos, mas também, pode representar para um mesmo utilizador, funções distintas, em momentos diferentes. Se a informação não tem toda o mesmo valor, isso implica que não irá ter necessidade de ser protegida toda da mesma maneira. Assim, diferentes tipos de informações devem ser protegidos de formas distintas. Para que isto seja possível, é necessário definir qual a informação que deve ser protegida, como e em que grau. Este processo de classificação é um dos primeiros passos num processo de implementação de uma política de segurança da informação.

Nesta perspectiva, a informação, enquanto resultado da interpretação de dados, está profundamente relacionada com os processos de recolha, análise, tratamento, armazenamento, e procedimentos de divulgação e destruição, questões que estão a ser alvo de grandes transformações fruto da nova geração de sistemas de armazenamento e de tecnologias inteligentes. Para uma melhor compreensão da ligação entre dados e informação, a mesma pode ser comparada à relação entre matéria-prima e produto final. Os dados são a matéria-prima que, após processados e organizados dão origem a um produto final, que permite a sua compreensão, classificação e utilização. É importante salientar que a classificação da informação, é um procedimento dinâmico, tendo em consideração que informações consideradas sigilosas em determinado período, podem numa data posterior passar a ser consideradas como informações passíveis de ser conhecidas pelo domínio público (Chopra & Chaudhary, 2020; Moura & Serrão, 2015; Piteira, Aparício, & Costa, 2019; Tawalbeh, Muheidat, Tawalbeh, & Quwaider, 2020).

Todos estes procedimentos que se incluem no conjunto organizado de elementos, constituído por dados, pessoas, *hardware*, *software*, redes de comunicação, que interagem entre si para processar informação, armazená-la e divulgá-la de forma adequada em função dos objectivos de uma organização denomina-se sistema de informação (SI) (Al-Mamary, Shamsuddin, & Aziati, 2014).

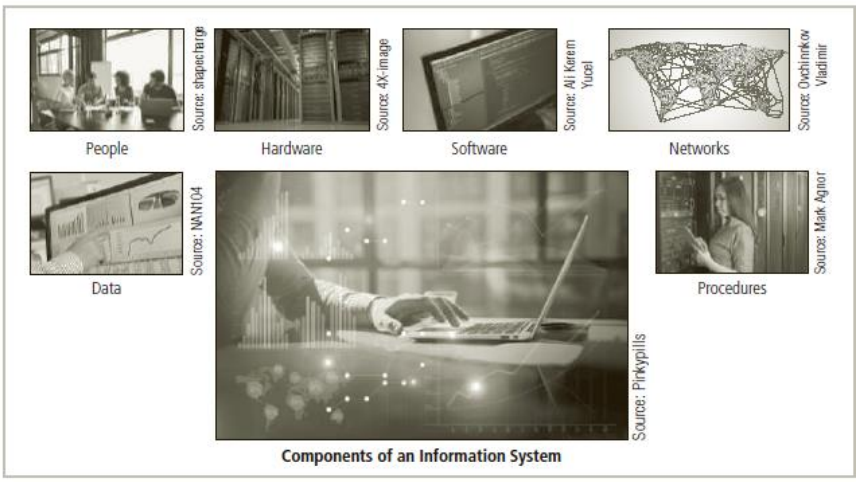
Embora os sistemas de informação de hoje sejam normalmente associados a algo que tem de ser realizado por meio de equipamentos informáticos, usamos sistemas de informação desde o início da civilização, como referem O'Brien e Marakas (2010) que explicam que a comunicação por sinais de fumo, também deve ser considerada como um sistema, e explicam que o termo sistema de informação tanto pode expressar um sistema automatizado, como um sistema manual.

No prisma empresarial, os sistemas de informação podem classificar-se de diversas maneiras, consoante a finalidade que irão apoiar no âmbito das operações ou da estratégia. Whitman e Mattord (2017) definem como componentes de um sistema de informação - *hardware*, *software*, redes, pessoas, procedimentos e os dados, sendo que a sua interacção permite que as informações sejam inseridas, processadas, geradas e armazenadas (figura 1). Cada um destes componentes do sistema de informação tem os seus próprios pontos fortes e fracos, bem como, as suas próprias características e utilizações. Cada componente tem igualmente requisitos específicos de segurança. A componente de s*oftware* são todos os aplicativos (programas), incorporada num equipamento e que possibilita ao mesmo executar as suas funções. Vão desde os sistemas operativos até às *apps* que se usam no dia a dia. Para estes autores o *software* é talvez a componente de um sistema de informação mais difícil de proteger e consideram que a exploração de erros na programação de software é responsável por uma parte substancial dos ataques à informação. As restrições frequentes de tempo, custos e mão-de-obra, condicionam uma visão de antecipação de vulnerabilidades e conduzem a posturas de intervenção tardias, com todos os inconvenientes inerentes. A componente *hardware* é a tecnologia física que acomoda e executa o *software*, armazena e transporta os dados e fornece interfaces para a entrada e remoção de informações do sistema. Whitman e Mattord (2017) descrevem que as políticas de segurança física lidam com o *hardware* como um activo físico e a lógica da protecção é através das ferramentas tradicionais de segurança física, como bloqueios e controlo de acesso. A evolução tecnológica nesta área tem sido muito grande, existindo cada vez mais soluções disponíveis no âmbito da biometria, do controlo por voz e por impressão digital. Relativamente aos dados os autores naturalmente que salientam que os mesmos devem ser armazenados, processados e transmitidos por um sistema de computador e em simultâneo protegidos. Os dados, para alguns autores são considerados como o activo mais valioso de uma organização em detrimento da informação, e, portanto, o principal alvo para ataques, revelando uma grande preocupação com a melhoria da segurança dos mesmos e dos aplicativos que os detêm. Não se pode correr o risco de ter bases de dados menos seguras do que o tradicional sistema de arquivos. Apesar de uma maior digitalização, muitas organizações continuam a deter muitos dados e informação na forma física, como relatórios em papel, apontamentos de reuniões, comunicações internas, informações sobre

dados dos parceiros, entre outros, pelo que a preocupação com a protecção deve ser idêntica ou maior do que a preocupação com a protecção de informações inseridas em computador, que normalmente, estão pelo menos salvaguardadas com controlo de acesso e sistemas de bloqueio. As Pessoas, são outra das componentes de um sistema de informação que muitas vezes não é contabilizada nas considerações sobre a segurança dos sistemas, representando uma enorme ameaça. Basta pensar que a espionagem é um conceito que existe desde os primórdios da civilização. No campo da espionagem organizacional tudo vale para se conseguir aquela informação que tanto se quer. Isto acontece porque muitas organizações consideram que obtêm vantagem sobre as suas rivais se obtiverem secretamente ideias inovadoras, se examinarem as condições de um contrato antes das negociações, ou se estiverem informadas sobre fusões e aquisições iminentes (Chopra & Chaudhary, 2020). A espionagem, não surgiu com o aumento da competitividade, ela é apenas um velho recurso que está a ser utilizado com novas técnicas e métodos. Tendo em consideração esta realidade, a apropriação indevida de dados e de informação pode ser realizada de forma intencional ou por mero acaso, o que impõe uma maior atenção ao desenvolvimento de uma política de conscientização sobre a pertinência da salvaguarda da confidencialidade e sigilo, mas também, de formação para evitar que os colaboradores, acidentalmente danifiquem ou percam informações. Relativamente aos procedimentos, estes consistem em instruções para realizar uma tarefa específica no sistema de informação e são um elemento essencial, mas por vezes, um pouco esquecido no âmbito da segurança. Quando alguém não autorizado obtém um procedimento de uma organização, este tipo de acontecimento, representa uma ameaça à integridade das informações, e consubstancia uma falha de segurança. Um pouco por todo o mundo, procedimentos de segurança negligentes causam perdas avultadas de dinheiro, antes da falha ser detectada e corrigida. Este facto ocorre essencialmente porque a maioria das organizações distribuem procedimentos aos funcionários para que eles possam aceder ao sistema de informação, mas muitas delas não fornecem a formação adequada, nem para a sua utilização, nem para a salvaguarda necessária em termos de segurança. Assim formar os funcionários sobre a protecção dos procedimentos é tão importante como proteger fisicamente o sistema de informação. Acresce ainda salientar que os procedimentos não devem ser difundidos por todos os funcionários, mas sim só para quem deles têm necessidade. Como último componente do sistema de informação, mas não menos importante Whitman e Mattord (2017) consideram a rede. Para estes autores é a rede que criou grande parte da necessidade de mais computadores e mais iniciativas de segurança da informação, nas organizações. Quando os sistemas de informação estão conectados entre si para formar uma rede de área local (LAN), e essa rede está conectada a outras redes, como a Internet, novos desafios de segurança emergem rapidamente. A tecnologia ligada em rede está cada vez mais disseminada em organizações de

todos os tamanhos, pelo que a definição de acessos e as opções para o efeito são de crucial importância na vida das organizações, e é preciso ter em consideração que os tradicionais controlos de acessos baseados em bloqueio e passwords podem não ser suficientes (Whitman & Mattord, 2017).

Figura 1 – Componentes de um Sistema de Informação



Fonte: Whitman & Mattord (2017, p.20)

Como síntese, em termos de contexto organizacional, a informação é cada vez mais considerada como o recurso mais valioso, porque descreve os recursos físicos, mas também, a sua envolvente interna e externa. A posse de recursos físicos sem informação sobre as suas características e utilidade, condiciona o seu aproveitamento e utilização eficaz, mas a informação não se circunscreve ao campo operacional da empresa, sendo o seu potencial de utilização estratégica enorme. A utilização da informação numa visão estratégica, permite às organizações antecipar e reagir mais rapidamente que a concorrência face a qualquer mudança da envolvente externa, bem como, criar vantagens competitivas, pela criação de valor através da afectação adequada de recursos na envolvente interna. Assim, a informação é um activo diferente de todos os outros, não se deprecia com o uso e pode aumentar de valor quando partilhada (Baskerville & Dhillon, 2008; Choo, 2003).

No entanto, a realidade das organizações é dinâmica e a necessidade de informação para apoio às diferentes situações de tomada de decisão também, e neste âmbito, a evolução tecnológica tem possibilitado que muitas actividades complexas e exaustivas fiquem mais fáceis e acessíveis, contudo, a própria evolução tecnológica é igualmente responsável pelo crescimento das preocupações com a segurança da informação (House, 2017; Watkins, 2008).

2.2 Os princípios de segurança da informação

Desde os anos 60 que a definição de segurança da informação está associada à confidencialidade, integridade e disponibilidade, a chamada tríade da CIA (*confidentiality, integrity, and availability*), no entanto, nos últimos anos alguns autores incluíram um conjunto vasto de possíveis acontecimentos, nomeadamente, danos acidentais ou intencionais, destruição, roubo, modificação não intencional ou não autorizada, ou outro uso indevido de ameaças humanas ou não humanas, como forma de garantir uma definição mais robusta e coerente com um novo ambiente organizacional mais complexo e interconectado (Furnell, Katsikas, Lopez, & Patel, 2008; Merkow & Breithaupt, 2014; Whitman & Mattord, 2017). Relativamente à confidencialidade, esta refere-se à capacidade de proteger os dados daqueles que não estão autorizados a consultá-los, a integridade consiste na capacidade de prevenir, recuperar e reverter alterações não autorizadas ou acidentais aos dados, a disponibilidade refere-se à possibilidade de acesso aos dados de pessoas autorizadas e em tempo útil (Cherdantseva & Hilton, 2012).

Para Whitman e Mattord (2017) o valor da informação advém das características que possui. Quando uma característica da informação muda, o valor dessa informação altera-se, podendo aumentar ou diminuir. Para estes autores, o que afecta o valor da informação é a existências de pontos críticos, como por exemplo, uma informação não ser disponibilizada no momento certo. Quando uma informação é disponibilizada tarde demais, pode perder valor, na medida em que deixou de ser útil e pertinente. Este aspecto é muito importante e deve estar presente na problemática que envolve a segurança, tendo em consideração que a segurança, tem como um dos propósitos a protecção do valor da informação.

Neste contexto, Whitman e Mattord (2017) definiram como características da informação: confidencialidade, integridade e disponibilidade e ainda, autenticidade, exactidão, utilidade e posse. A informação é autêntica quando está no mesmo estado em que foi criada, colocada, armazenada ou transferida. A autenticidade da informação é, por conseguinte, a qualidade ou estado de ser genuína ou original. Considera-se que a informação é exacta quando está livre de erros. Se as informações foram intencionalmente ou não modificadas, perdem a característica de exactidão. A utilidade da informação é a qualidade ou estado de ter valor para alguma finalidade. Por outras palavras, a informação tem valor quando pode servir a um propósito. Se a informação estiver disponível, mas não tem um formato significativo para o utilizador final, não é útil. A posse de informação é a qualidade ou estado de propriedade ou controle. Diz-se que a informação está na posse de alguém se esse alguém a detiver, independentemente do formato em que se encontra (Whitman & Mattord, 2017).

Merkow e Breithaupt (2014) definiram doze princípios para garantir o sucesso na segurança da informação, tendo como mensagem mais relevante que nada é cem por cento seguro, que a complexidade é inimiga da segurança e que a segurança deve ser construída numa visão de prevenção, detecção e correcção (quadro 1).

Quadro 1 – Princípios para garantir sucesso na segurança da informação

	Principles
1	There Is No Such Thing as Absolute Security
2	The Three Security Goals Are Confidentiality, Integrity, and Availability
3	Defense in Depth as Strategy
4	When Left on Their Own, People Tend to Make the Worst Security Decisions
5	Computer Security Depends on Two Types of Requirements: Functional and Assurance
6	Security Through Obscurity Is Not an Answer
7	Security = Risk Management
8	The Three Types of Security Controls Are Preventative, Detective, and Responsive
9	Complexity Is the Enemy of Security
10	Fear, Uncertainty, and Doubt Do Not Work in Selling Security
11	People, Process, and Technology Are All Needed to Adequately Secure a System or Facility
12	Open Disclosure of Vulnerabilities Is Good for Security!

Fonte: Merkow e Breithaupt (2014, p.19-30)

No quadro 2 apresentam-se as definições de segurança da informação apresentadas pela *International Organization for Standardization* (ISO) pelo *Committee on National Security Systems* (CNSS) e pelo *Information Systems Audit and Control Association* (ISACA).

Quadro 2 - Definições de Segurança da Informação

ISO	Preservation of confidentiality, integrity and availability of information. Note, in addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.
CNSS	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
ISACA	Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability).

Fonte: Adaptado de Cherdantseva & Hilton (2012, p.29)

Em 2018 a ISO (*The International Organization for Standardization*) e a IEC (*The International Electrotechnical Commission*) publicaram uma actualização das normas ISO/IEC 27000 com o propósito de ajudar as organizações a manter os seus activos de informação seguros,

nomeadamente, as informações financeiras, os dados pessoais dos colaboradores, dos clientes e dos demais parceiros, bem como, toda a informação que lhe for confiada (Watkins, 2008).

Assim, e se para maximizar a utilidade da informação, esta deve ser gerida adequadamente tendo em consideração a sua classificação e especificidades, tal como acontece com os outros recursos, não é possível falar em gestão eficaz, sem que a informação esteja devidamente segura, em todo o ciclo da informação desde a recolha, passando pelo armazenamento e formas de acesso, distribuição ou mesmo a sua destruição. Todo este processo deve estar em sintonia com os objectivos da organização e o tipo de negócio (Baskerville & Dhillon, 2008).

Como síntese, proteger as informações em contexto organizacional é um grande desafio e inclui conhecer os riscos da envolvente interna e da envolvente externa. Em termos das questões internas, a cultura organizacional expressa em termos de visão, missão e valores, nas políticas, estratégias de negócios e objectivos, pode ajudar a definir uma política de segurança da informação. Na implementação de uma cultura de segurança os recursos disponíveis são também muito importantes, quer os materiais, como tecnologias, sistemas e equipamentos, quer os comportamentos e formação dos humanos, enquanto colaboradores. Relativamente à envolvente externa, é fundamental cumprir todos os requisitos de segurança legislativos e dispor de controlos adequados para evitar a apropriação indevida, a manipulação, ou destruição por terceiros de dados ou informação, e ainda, numa perspectiva de antecipação e vigia estratégica estar alerta sobre as tendências tecnológicas (House, 2017). As novas tecnologias tanto podem trazer mecanismos de maior segurança, como podem exigir novas formas de proteger os dados e as informações, nos sistemas existentes. Um suporte tecnológico obsoleto pode-se tornar mais vulnerável (Chopra & Chaudhary, 2020).

2.3 A integridade como princípio de segurança da informação

A integridade da informação consiste em garantir que os dados disponíveis são exactos e confiáveis e não foram modificados, alterados ou destruídos, quer de forma propositada, quer de forma acidental. O conceito de integridade refere-se assim à capacidade de manter as características originais dos dados e da informação. A integridade dos dados ou da informação pode ser comprometida por diferentes formas, razão pela qual representa um aspecto crucial num protocolo de segurança (Trites, 2013). Assim, uma informação é considerada íntegra quando se mantém fiel às suas características originais e o receptor tem acesso exactamente à mensagem enviada pelo emissor. Se, por exemplo, uma mensagem de e-mail for interceptada e tiver seu conteúdo alterado, considera-se que tem a integridade comprometida. O comprometimento da

integridade pode ter origem num acto intencional ou acidental, e este ser cometido por erro humano, falha dos equipamentos, incompatibilidade de software, *bugs*, vírus, *malware*, *hacking* e outras ameaças cibernéticas (Whitman & Mattord, 2017, Trites, 2013).

É importante destacar que a informática se desenvolveu muito nas últimas décadas e de uma ferramenta administrativa, cujo objectivo era optimizar processos, tornou-se num instrumento estratégico para as organizações; e a segurança da informação transformou-se num requisito vital das organizações, tendo em consideração que as operações passaram a ser suportadas em algum tipo de tecnologias de informação e comunicação (Flowerday & Solms, 2005). Neste sentido, as organizações deixaram de ter como opção a não segurança da informação, e passaram a ter como necessidade a avaliação do risco numa visão holística, dado que um sistema pode ter integridade, mas se os dados e a informação carecem de integridade, no momento em que o sistema os recebe continuaram a não ter integridade e, por conseguinte, não podem ser considerados como confiáveis, mesmo que o sistema o seja (Ward & Peppard, 2002).

Assim, o valor da informação advém da sua relevância e utilidade, mas igualmente da sua integridade. A integridade é a garantia da exactidão da informação e dos métodos de processamento. Da mesma forma que um relatório financeiro de uma empresa deve ser fiel em cada número apresentado, o conteúdo de uma base de dados deve ser mantido inalterado.

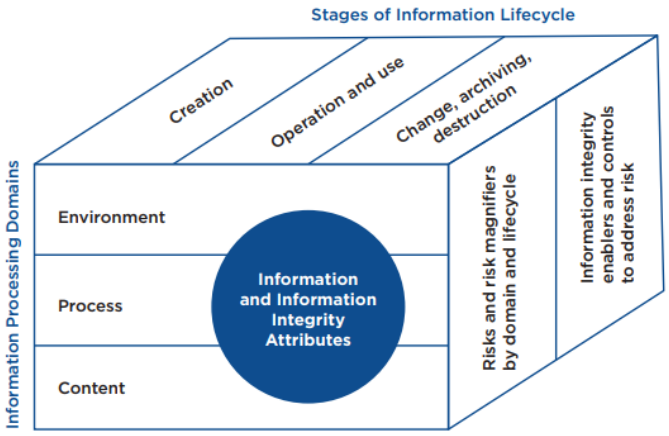
Boritz *et al*. (2019) explica que a integridade da informação é traduzida pela consistência da informação e pela sua *representational fidelity*, e dá como exemplo que durante a crise financeira de 2008, os títulos anteriormente classificados como AAA tiveram que ser rebaixados dezasseis posições, o que sugere que a classificação atribuída de AAA carecia de *representational fidelity*, dado que era inconsistente com o risco financeiro real dos mesmos.

No modelo desenvolvido por Boritz *et al*. (2019) a *representational fidelity* é analisada segundo quatro atributos, que os autores consideram como os principais: validade, integridade, actualidade e precisão e a estrutura de integridade da informação engloba os seguintes componentes: (i) informações e os atributos da sua integridade, (ii) o ciclo de vida da informação, (iii) domínios de processamento de informações (ambiente, processo e conteúdo), (iv) riscos de integridade da informação e ampliadores de risco, (v) facilitadores da integridade da informação e (vi) controles projectados para lidar com os riscos.

O ciclo de vida da informação pressupõe um diagnóstico das necessidades de informação e dos instrumentos imprescindíveis para responder a essas necessidades, e deverá ser adequado à estrutura e modelo de gestão da organização, pelo que é importante conhecer quais as funções da

organização, como as decisões são tomadas, como é divulgada a informação e quais os objectivos estratégicos da mesma. A figura 2 apresenta o ciclo de vida da informação dividido em três fases: *creation*; *operation and use*, e *change, archiving or destruction* e identifica três domínios de processamento de informação que afectam a integridade: *content*; *processing*; e *information system* (IS) *environment*. Estes três domínios (*content*; *processing*; e *information system* (IS) *environment*) têm riscos de integridade de informação diferentes e sobrepostos, que devem ser mitigados e controlados. Os riscos são maiores ou menores consoante as características de cada ciclo de vida da informação, a natureza do sistema de informação, a complexidade dos processos e o próprio sector de actividade da organização (Boritz *et al*., 2019).

Figura 2 - Framework de Integridade da Informação



Fonte: Boritz *et al*. (2019)

2.4 Factores e dimensões do risco, das ameaças e das vulnerabilidades

A evolução dos procedimentos e da tecnologia, no âmbito da recolha, tratamento e armazenamento da informação, de que são exemplos as técnicas de mineração, o recurso à inteligência artificial, ou a *Cloud*, têm contribuído para a construção de um novo olhar sobre a gestão do risco nos mercados e por inerência, sobre a gestão do risco organizacional. Neste contexto, o risco pode ser definido como a probabilidade de que algo prejudicial aconteça a um activo (Kim & Solomon, 2018) e a gestão do risco organizacional como o conjunto de iniciativas e decisões que visam proteger os activos e melhorar o desempenho, através da definição de critérios e procedimentos construídos sobre uma orientação de probabilidade de ocorrência e quantificação de impactos (Otero, 2019). Cumpre destacar que no contexto da segurança de TI, um activo pode ser hardware, software, base de dados, arquivos ou a própria rede física (Kim & Solomon, 2018).

Na verdade, num mundo em constante mutação a análise dos diferentes tipos de risco, quer da envolvente externa, quer da envolvente interna, deve ser um dos propósitos do planeamento estratégico, numa óptica de monitorização e controlo, mas também de antecipação, mesmo sabendo que não é possível estar totalmente seguro (House, 2017; Saffady, 2021).

Quer na nossa vida, como na vida de uma empresa o risco existe, logo, o que é necessário decidir é qual a tolerância ao risco, isto é, o que se considera aceitável, e para o efeito é indispensável conhecer os seus factores e dimensões de ameaças e vulnerabilidades. Um processo de gestão de risco deve identificar e descrever ameaças, identificar e avaliar vulnerabilidades e avaliar opções de resposta ao risco, porque riscos não reconhecidos não podem ser geridos (Saffady, 2021). Portanto, a política de segurança da informação deve ser construída com base nas avaliações de risco e num equilíbrio entre a utilidade do uso da informação e o risco das ameaças (House, 2017). Uma avaliação de risco confiável e objectiva permite que as organizações desenvolvam um plano para mitigar, prevenir ou eliminar ameaças potenciais, mas também, antecipar precocemente vulnerabilidades e criar soluções automatizadas específicas de melhoria (Igried, Al-Wahshat, Igried, & Takialddin, 2019).

Kim e Solomon (2018) referem que riscos, ameaças e vulnerabilidades "caminham juntos", e que enquanto o risco é a probabilidade de algo acontecer, uma vulnerabilidade é uma fraqueza que permite que uma ameaça seja percebida ou tenha um efeito sobre um activo, considerando como ameaça qualquer acção que pode danificar ou comprometer um activo. Em suma, uma vulnerabilidade que pode ser explorada é uma ameaça. Se existe uma vulnerabilidade num sistema, analogamente existe a possibilidade de uma ameaça. Qualquer ameaça contra uma vulnerabilidade cria o risco de que um evento negativo possa acontecer. Não sendo possível eliminar as ameaças, é possível criar condições para proteger a informação contra vulnerabilidades. Dessa forma, mesmo que uma ameaça ainda exista, ela não pode explorar a vulnerabilidade. A chave para proteger os activos do risco de ataque é eliminar ou abordar tantas vulnerabilidades quanto possível. As ameaças podem ter origem interna ou externa, intencional ou acidental e podem ser praticadas por um indivíduo, um grupo de indivíduos ou uma outra organização e devem ser identificadas e classificadas de acordo com sua importância e impacto (Saffady, 2021). Identificar e responder a ameaças e vulnerabilidades não é um processo fácil, mas é essencial. Em certas ocasiões, uma ameaça pode ser muito dispendiosa ou demorada para eliminar, pelo que Kim e Solomon (2018) recomendam que o objectivo deve ser reduzir ao mínimo possível as ocorrências e que se deve ponderar cuidadosamente se o custo de proteger alguns activos não é maior do que o valor dos próprios activos. O quadro 3 apresenta uma lista das ameaças e vulnerabilidades mais comuns nos sete domínios de uma infraestrutura de TI.

Quadro 3 - Ameaças e vulnerabilidades comuns nos sete domínios de uma infraestrutura de TI

Domain	Common Threats And Vulnerabilities
User domain	Lack of awareness or concern for security Accidental acceptable use policy violation Intentional malicious activity Social engineering
Workstation domain	Unauthorized user access Malicious software introduced Weaknesses in installed software
LAN domain	Unauthorized network access Transmitting private data unencrypted Spreading malicious software
LAN-to-WAN domain	Exposure and unauthorized access to internal resources from the outside Introduction of malicious software Loss of productivity due to lack of Internet access
WAN domain	Transmitting private data unencrypted Malicious attacks from anonymous sources Denial of service attacks Weaknesses in software
Remote Access domain	Brute-force password attacks on access and private data Unauthorized remote access to resources Data leakage from remote access or lost storage devices
System/Application domain	Unauthorized physical or logical access to resources Weaknesses in server operating system or application software Data loss from errors, failures, or disasters

Fonte: Kim & Solomon (2018, p.88)

Em termos de tipologia de ameaças Kim e Solomon (2018) consideram três realidades: (i) Ameaças de divulgação, (ii) Ameaças de alteração e (iii) Ameaças de perda ou destruição. Uma ameaça de divulgação ocorre quando utilizadores não autorizados acedem a informações privadas e confidenciais. A divulgação dessa informação pode afectar os resultados da actividade empresarial, comprometer a continuidade do negócio e violar legislação em vigor, configurando crime de falta de protecção adequada dos dados, com repercussões financeiras e de imagem para a organização. Este tipo de ameaça é de extrema importância porque não pode ser corrigido. Depois de alguém visualizar dados confidenciais não existe a possibilidade de os remover da sua memória. Assim, os dados estão seguros quando só estão disponíveis para utilizadores autorizados e não estão acessíveis a utilizadores não autorizados. Garantir este controlo ajuda também a salvaguardar outros aspectos da segurança da informação. Uma ameaça de alteração viola a

integridade da informação. Este tipo de ataque compromete um sistema, fazendo alterações não autorizadas aos dados, intencionalmente ou não. Esta mudança pode ocorrer enquanto os dados são armazenados num recurso de rede ou enquanto são transferidos. As alterações intencionais geralmente são maliciosas, enquanto que as alterações não intencionais são geralmente acidentais. Uma das formas mais comuns na tipologia de alteração acidental são os erros cometidos pelas pessoas, os quais afectam a integridade dos dados e representam um problema de segurança. Modificações na configuração do sistema igualmente podem comprometer a integridade da informação, pelo que é importante implementar técnicas que permitam acompanhar as consequências da mudança, através do registo de quem, o quê, quando, onde e como as modificações foram feitas. Ter uma cópia sistematicamente actualizada dos dados (backup) também pode reduzir a gravidade de uma ameaça de alteração. Um backup também pode diminuir o impacto de uma ameaça de perda ou destruição. A ameaça de perda ou destruição, torna a informação indisponível ou inutilizável e viola o princípio em termos de segurança da disponibilidade.

O quadro 4 apresenta as ameaças mais comuns nos sete domínios de uma infraestrutura de TI.

Quadro 4 - Alvos de ameaças nos sete domínios de uma infraestrutura de TI

Domain	Threat targets
User domain	Employees' own human traits and behavior. Violations of the acceptable use policy are targeted
Workstation domain	Workstations, laptops, and mobile devices are the target, along with their vulnerabilities. This domain is the point of entry into the IT infrastructure
LAN domain	Windows Active Directory/Domain Controllers, file servers, print servers. In addition, the IP data network is part of the LAN domain and is a target for ID and authentication attacks.
LAN-to-WAN domain	DMZ VLANs or dedicated remote connections are typically terminated here. Public-facing IP devices, including perimeter security with firewalls, IDS/IPS, and remote VPN terminations, reside here.
WAN domain	IP routers, TCP/IP stacks and buffers, firewalls, gateways, switches, and WAN service providers are targeted.
Remote Access domain	Virtual private networks (VPNs), two-factor authentication, and remote access for mobile workers and teleworkers are typically supported and targeted.
System/Application domain	Web and application servers, operating systems, and applications. Back-end database servers and database tables with sensitive data are the target.

Fonte: Kim & Solomon (2018, p.90)

Sinnett (2008) analisou várias empresas que receberam o Prémio de Excelência da Integridade da Informação *The IIC's Excellence in Information Integrity Award*, de 1995 a 2007, tendo observado que o esforço para alcançar a integridade da informação é cada vez mais valorizado pelos acionistas, funcionários, reguladores e outras partes interessadas. Este autor utilizou três empresas – Steria; Swedbank e Wal-Mart para ilustrar as suas recomendações para melhorar a integridade da informação (quadro 5).

Quadro 5 - Lições a retirar dos Estudos de Caso

Company	Lessons from the Case Studies
Steria	• Involve senior management in information integrity initiatives to emphasize that the project is a top priority. • Standardize systems on a common technology platform and use a common chart of accounts. • Processes should be automated, which will result in increased control and reduction of manual intervention and errors. • Quality standards can be assured and maintained through rigorously applied Service Level Agreements and Key Performance Indicators.
Swedbank	• Implement software that will automatically detect errors. • Detection software should replace manual controls.
Wal-Mart	• Use date warehouses to provide information for special projects as well as routine business activities. • Develop information networks which can synchronize information that may be shared with customers. • Promote customer convenience with the use of centralized databases.

Fonte: Sinnett (2008, p.17)

2.5 A informação e a tomada de decisão: a importância da gestão do risco

Vários factores intervêm no processo da tomada de decisão, sendo um deles a informação. Neste sentido, a informação tem de acompanhar a gestão das operações e alicerçar a tomada de decisão, em conformidade com as necessidades da organização, as quais são dinâmicas e multifacetadas. É interessante destacar que a gestão da informação não é contemporânea dos nossos dias, pelo que basta recuar a qualquer situação de guerra da história da humanidade para perceber a importância da articulação da informação, perante um número sempre elevado de indivíduos. Assim, e para responder a um contexto cada vez mais complexo e de desafios crescentes no âmbito das ameaças, a gestão de risco em TI, é a pedra angular para a tomada de decisões assertivas e para a comunicação e partilha em segurança dentro das organizações, e na sua relação com o exterior.

Como explicam Kure, Islam e Razzaque (2018), o risco pode ser definido como um evento incerto que pode ocorrer devido a um mau funcionamento ou falha do sistema que podem prejudicar os activos e também condicionar a concretização dos objectivos estratégicos, operacionais e financeiros, enquanto que, a sua gestão é a chave para identificar e avaliar os

potenciais riscos de forma integrada em todos os níveis de uma organização para permitir a definição de prioridades e minimização dos mesmos. Os métodos tradicionais de avaliação de risco de segurança abordam apenas risco de segurança de TI ou risco de conformidade, mas uma gestão integrada do risco construirá uma estrutura numa visão holística, considerando os aspectos técnicos e não técnicos da organização, de modo a salvaguardar a necessidade de prevenção, detecção e recuperação, resiliência e dissuasão de ataques (Kure *et al*.,2018). A consideração de uma organização de forma integrada é essencial em virtude das organizações estarem, cada vez mais, dependentes dos recursos e ferramentas tecnológicas. Dashti, Giorgini e Paja, (2017) referem que existem duas razões principais para as organizações falharem na análise de risco: (i) planos de risco incompletos, e (ii) priorização ineficaz do risco, isto é, colocar o foco num único critério, como por exemplo o impacto financeiro, em detrimento de uma combinação de critérios quantitativos e qualitativos.

Para utilizar a informação com eficácia e eficiência na tomada de decisão é fundamental que a gestão do risco tenha como propósito assegurar uma comunicação eficaz e segura. Neste sentido, a gestão de risco, deve ser um processo contínuo e que flui através da organização, conduzida por profissionais em todos os níveis e aplicada a todos as unidades, ou departamentos, numa visão de portfólio de todos os riscos a que a organização está exposta, previstos e imprevistos e deve ser formulada para identificar eventos em potencial, com base em duas perspectivas: probabilidade e impacto (Steinberg, Marte

Alhalafi, N., & Veeraraghavan, P. (2019). Privacy and Security Challenges and Solutions in IOT: A review. *International Conference on Smart Power & Internet Energy Systems.*, *322*, p. 012013. doi:10.1088/1755-1315/322/1/012013

Al-Mamary, Y. H., Shamsuddin, A., & Aziati , N. (2014). The Role of Different Types of Information Systems In Business Organizations : A Review. *International Journal of Research (IJR), 1*(7), pp. 1279-1286.

Augusto, A. (2014). Metodologias quantitativas/metodologias qualitativas: mais do que uma questão de preferência. *Forum Sociológico Série II, 24*, pp. 1-9. doi:10.4000/sociologico.1073

Bapty, T., & al., e. (2017). *Handbook of Sysrem Safety and Security. Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems.* United States: Elsevier Inc.

Boeckl, K., & et al. (2021). *Considerações para Gerenciar Riscos de Privacidade e Segurança Cibernética na Internet das Coisas (IoT). NIST Interagency/Internal Report (NISTIR) - 8228pt*. Gaithersburg: National Institute of Standards and Technology (NIST).

Boritz, J. E., & et al. . (2019). *A Framework for Information Integrity Controls.* Canada: Chartered Professional Accountants of Canada (CPA Canada).

Brandão, P. R., & Rezende, M. (2020). Data: The most valuable commodity. *Kriativ.tech, 8*(1), pp. 1-7. doi:10.31112/kriativ-tech-2020-08-47

Cabral, A. d., Bianchi, M., & Gyenge , F. (2018). *Glossário De Termos Técnicos de T.I* (4ª ed.). São Paulo: Editora Senac .

Cherdantseva, Y., & Hilton, J. (2013). A Reference Model of Information Assurance & Security. *Conference: Availability, Reliability and Security (ARES), 2013 Eighth International Conference on Project: Secure*BPMN* (pp. 546-555). Regensburg, Germany: IEEE. doi:10.1109/ARES.2013.72

Chopra, A., & Chaudhary, M. (2020). *Implementing an Information Security Management System. Security Management Based on ISO 27001 Guidelines.* New York: Springer Science+Business Media New York. doi:10.1007/978-1-4842-5413-4

Creswell, J. W. (2014). *Research design : qualitative, quantitative, and mixed methods approaches* (4th ed.). United States of America: SAGE Publications, Inc.

Dashti, S., Giorgini, P., & Paja, E. (2017). Information Security Risk Management. *10th Conference: IFIP Working Conference on The Practice of Enterprise Modeling* (pp. 18-33). Leuven, Belgium: Springer. doi:10.1007/978-3-319-70241-4_2

Flowerday, S., & Solms, R. (2005). Real-time information integrity=system integrity+data integrity+continuous assurances. *Computers & Security, 24*, pp. 604-613. doi:10.1016/j.cose.2005.08.004

Furnell, S. M., Katsikas, S., Lopez, J., Patel, A., & Editors. (2008). *Securing Information and Communications Systems. Principles, Technologies, and Applications.* Norwood, United States of America: Artech House, Inc.

Griffor, E. (2017). *Handbook of System Safety and Security. Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems.* United States of America: Elsevier Inc.

House, N. (2017). *The Complete Cyber Security Course* (Vol. I). London: StationX Ltd.

Igried, A.-K., Al-Wahshat, H., Igried, B., & Takialddin, A.-S. (2019). Risk and Vulnerability Analyses for the protection of Information for Future communication security Based Neural Networks. *Journal of Advanced Sciences and Engineering Technologies, 2*(1), pp. 31-39. doi:10.32441/jaset.02.01.03

INFORMA. (2021). *Diretório de todas as empresas portuguesas*. Retrieved Maio 26, 2021, from Informa D&B Portugal: https://diretorio.informadb.pt/

Kim, D., & Solomon, M. (2018). *Fundamentals of information systems security* (3rd ed.). United States of America: Jones & Bartlett Learning.

Kure, H. I., Islam, S., & Razzaque, M. (2018). An Integrated Cyber Security Risk Management. Approach for a Cyber-Physical System. *Applied Sciences, 8*(898), pp. 1-29. doi:10.3390/app8060898

Laudon, K. C., & Laudon, J. (2018). *Management Information Systems. Managing the Digital Firm.* England: Pearson Education Limited.

Leavy, P. (2017). *Research Design. Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches.* New York: Guilford Publications, Inc.

Leeuw, K. M., & Bergstra, J. (2007). *The History of Information Security. A Comprehensive Handbook.* Netherlands: Elsevier B.V. doi:10.1016/B978-0-444-51608-4.X5000-7

Magalhães, M., & Hill, A. (2008). *Investigação por Questionário* (2ª ed.). Lisboa: Edições Sílabo.

Merkow, M. S., & Breithaupt, J. (2014). *Information Security: Principles and Practices.* United States of America: Pearson Education, Inc.

National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1.* USA: National Institute of Standards and Technology (NIST). doi:10.6028/NIST.CSWP.04162018

O'Brien, J. A., & Marakas, G. (2010). *Introduction to Information Systems* (15th ed.). New York: McGraw-Hill/Irwin.

Orvalho, L., Figueiredo, B., & Pinto, H. (2020). IoT e Internet 5G. *Kriativ.tech*, pp. 1-6. doi:10.31112/kriativ-tech-2018-01-22

Otero, A. R. (2019). *Information Technology Control and Audit* (5th ed.). Florida: Taylor & Francis Group, LLC.

Piteira, M., Aparicio, M., & Costa, C. (2019). A Ética na Inteligência Artificial: Desafios. *CISTI'2019 - 14ª Conferência Ibérica de Sistemas e Tecnologias de Informação* (pp. 1-6). Coimbra: AISTI - Associação Ibérica de Sistemas e Tecnologias de Informação.

Pordata. (2020). *População empregada: total e por profissões*. Retrieved Maio 20, 2021, from Emprego e Mercado de Trabalho: https://www.pordata.pt/Portugal/Popula%c3%a7%c3%a3o+empregada+total+e+por+profiss%c3%b5es-3385

Quivy, R., & Campenhoudt, L. (2018). *Manual de Investigação em Ciências Sociais.* Lisboa: Gradiva.

Rees, J., Bandyopadhyay, S., & Spafford, E. (2003). PFIRES: A Policy Framework for Information Security. *Communications of the Association for Computing Machinery (ACM)*, pp. 1-18. doi:10.1145/792704.792706

Risk and Vulnerability Analyses for the protection of Information for Future communication security Based Neural. (n.d.).

Saffady, W. (2021). *Managing Information Risks: Threats, Vulnerabilities, and Responses.* United Kingdom: Rowman & Littlefield Publishers.

Safianu, O., Twum, F., & Hayfron-Acquah, J. (2016). Information System Security Threats and Vulnerabilities: Evaluating the Human Factor in Data Protection. *International Journal of Computer Applications, 143*(5), pp. 8-14. doi:10.5120/ijca2016910160

Sinnett, W. M. (2008). *Excellence in Information Integrity.* United States of America: Financial Executives Research Foundation.

Sperstad, I. B., Kjølle, G., & Gjerde, O. (2020). A comprehensive framework for vulnerability analysis of extraordinary events in power systems. *Reliability Engineering and System Safety, 196*, p. 106788. doi:10.1016/j.ress.2019.106788

Steinberg, R. M., Martens, F., Everson, M., & Nottingham, L. (2007). *Gerenciamento de Riscos Corporativos – Estrutura Integrada: Sumário Executivo e Estrutura.* USA: Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Straub, D. W., Goodman, S., & Baskerville , R. (2008). *Information Security. Policy, Processes, and Practices.* United States of America: M.E. Sharpe, Inc. doi:10.1016/B978-0-444-51608-4.X5000-7

Susanto, H., & Almunawar, M. (2018). *Information Security Management Systems. A Novel Framework and Software as a Tool for Compliance with Information Security Standards.* (I. Apple Academic Press, Ed.) Canada: Taylor & Francis Group,LLC.

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions. *Applied Sciences, 10*(12), pp. 1-17. doi:10.3390/app10124102

The Institute of Internal Auditors, Inc., ("The IIA"). (2016). *Global Perspectives: A Auditoria Interna como Conselheira Confiável de Cibernética.* Lake Mary, USA: The Institute of Internal Auditors, Inc., ("The IIA").

The Institute of Internal Auditors, Inc., ("The IIA"). (2019). *Global Perspectives and Insights. 5G e a Quarta Revolução Industrial (Parte 1).* Lake Mary, USA: The Institute of Internal Auditors, Inc., ("The IIA").

Trites, G. (2013). *Information Integrity.* United States: American Institute of Certified Public Accountants (AICPA).

Vilelas, J. (2017). *Investigação. O processo de Construção do Conhecimento* (2ª ed.). Lisboa: Edições Sílabo.

Ward, J. L., & Peppard, J. (2002). *Strategic Planning for Information Systems* (3rd ed.). United Kingdom: John Wiley & Sons Ltd.

Watkins, S. G. (2008). *An Introduction to Information Security and ISO27001. A Pocket Guide.* United Kingdom: IT Governance Publishing.

Whitman, M. E., & Mattord, H. (2017). *Principles of Information Security* (6th ed.). United States of America: Cengage Learning.

ns, Everson, & Nottingham, 2007).

Em suma, sempre que existe o risco de uma vulnerabilidade poder ser explorada, estamos perante uma ameaça, que pode ser classificada em: ameaças de divulgação, ameaças de alteração e ameaças de perda ou destruição, com origem internas ou externas, acidentais ou intencionais, realizadas por ser humano ou por dispositivos. Como não é exequível garantir 100% de segurança num sistema, a integridade da informação é, actualmente, um dos principais problemas na tomada de decisão e por inerência na gestão das organizações. Por conseguinte, a gestão de risco, incluindo um sistema de controles internos, tornou-se fundamental para garantir a integridade da informação e a sua utilização em tempo real, quer em termos estratégicos, quer operacionais.

PARTE II – Prática

Capítulo 3 – Metodologia

3.1 Opções metodológicas

O presente estudo tem como propósito o desenvolvimento de uma *framework* de análise das vulnerabilidades de um sistema de informação, com o objectivo de identificar potenciais ameaças e mitigar riscos. Para concretizar este propósito o estudo foi desenvolvido com cariz descritivo, abordagem quantitativa baseada em inquérito por questionário, elaborado para o efeito e desenhado em cinco etapas (Creswell, 2014).

Na primeira, e com base na revisão bibliográfica foram identificados alguns conceitos e

abordagens considerados de referência para a compreensão do tema da segurança da informação, com especial relevo para a problemática da integridade e da necessidade de implementar uma cultura de comportamentos seguros, na utilização de dados e informação por parte dos colaboradores. Na segunda etapa, procurou-se fazer emergir as variáveis que mais interferem com a segurança e integridade da informação e que são passíveis de abordagem quantitativa, tendo as mesmas sido agrupadas por domínios e subdomínios. Na terceira etapa elaborou-se um questionário, realizou-se um pré-teste para validação da coerência e clareza do mesmo, e procedeu-se à recolha e tratamento dos dados. Na quarta etapa e com base nos resultados obtidos desenvolveu-se uma *framework* de análise das vulnerabilidades de um sistema de informação. Na quinta etapa, e tendo como alicerce o trabalho desenvolvido nas etapas anteriores, apresentam-se as conclusões finais e recomendações.

A escolha de um estudo descritivo é justificada, tendo em consideração que este tipo de estudos, visam avaliar diferentes aspectos, dimensões ou componentes de um fenómeno ou fenómenos a investigar, sem interferir. Caracterizam-se habitualmente como estudos que procuram conhecer opiniões e comportamentos. Como refere ainda Vilelas (2017) a grande valorização dos estudos descritivos assenta na premissa que os problemas podem ser resolvidos e as práticas melhoradas através do conhecimento, construído pela descrição e análise de resultados obtidos e observados na investigação dos fenómenos.

A opção pelo estudo quantitativo, tem como alicerce motivos de carácter operacional, mas também, de maior objectividade, precisão e facilidade de tratamento estatístico, dado que se privilegiou conhecer o fenómeno em estudo e não a opinião dos inquiridos sobre o fenómeno em estudo (Leavy, 2017). As abordagens quantitativas e qualitativas diferem, assim, nos seus fundamentos filosóficos, nos princípios que inspiram e conduzem a investigação, ou seja, na metodologia, mas também, nos instrumentos e técnicas de investigação (Augusto, 2014). No entanto, cada vez mais são considerados como não antagónicos, e neste sentido, passíveis de serem utilizados em simultâneo face à sua complementaridade (Leavy, 2017). No presente caso e dado que o cerne da investigação é o desenvolvimento de uma *framework* de análise das vulnerabilidades de um sistema de informação, com o objectivo de identificar potenciais ameaças e mitigar riscos, a opção não se evidenciou como a mais pertinente, apesar do rigor que ambas as abordagens podem incorporar. Neste sentido, a opção pela abordagem quantitativa, foi ponderada em função da opção mais adequada para a concretização dos objectivos da presente pesquisa. Como explica Augusto (2014, p,2):

> "A opção por uma metodologia quantitativa ou qualitativa tem de estar de acordo tanto com os objectivos da pesquisa como com os atributos dos objectos em estudo. Não é, por isso, possível colocar os métodos de

> pesquisa numa hierarquia de excelência, dado que diferentes métodos são apropriados para responder a diferentes propósitos e questões de investigação".

Como principais vantagens da opção quantitativa destacam-se a objectividade, o facto de impor um método de recolha de informação estruturado, permitir uma medição padronizada, numérica, e com possibilidade de tratamento estatístico.

3.2 Objectivos e questões de investigação

Como recomenda Leavy (2017), o objectivo deve permitir uma visão global e abrangente do tema de pesquisa, e está intrinsecamente relacionado com o problema principal ou fenómeno em estudo. Neste sentido, foi definido como objectivo: conhecer o tipo de informação interna e externa mais valorizado e utilizado pelas organizações, quais as tecnologias e procedimentos de protecção incorporados e quais os principais constrangimentos por elas já identificados. Tendo em consideração que uma investigação é algo que se procura, é recomendada a formulação de uma ou mais questões, através das quais seja possível exprimir e clarificar o mais exactamente possível o que se procura saber, verificar ou compreender melhor. Por conseguinte, as questões devem ser precisas concisas, para deterem clareza, devem ser realistas, em termos de recursos seja de conhecimento, seja de tempo, ou materiais, para serem exequíveis e devem ser pertinentes (Quivy & Campenhoudt, 2018). Neste sentido, foram definidas como linhas condutoras da investigação as seguintes questões: (i) analisar se a informação recolhida pelas organizações está devidamente protegida e com que procedimentos? (ii) se a informação armazenada está protegida e salvaguardada a sua integridade? (iii) como são geridos os acessos da informação recolhida e armazenada pelas organizações? (iv) se as novas tecnologias de armazenamento e processamento são uma ferramenta cada vez mais utilizada pelas organizações?

3.3 Procedimentos e instrumentos de recolha da informação

Para a elaboração do questionário foi tida em consideração a revisão bibliográfica em geral, e em particular o contributo dos autores apresentados no quadro 6, as recomendações do *National Institute of Standards and Technology* (NIST) e das *International Organization for Standardization* (ISO).

No caso de Saffady (2021) estamos perante uma obra que atribui especial relevo à gestão do risco e à importância da sua identificação, análise e controlo enquanto ameaça aos activos, incluindo os activos de informação.

Sperstad *et al*. (2020) analisam diferentes factores que influenciam a vulnerabilidade em sistemas de energia, dividindo os factores em três categorias: factores técnicos, factores humanos

no âmbito dos operadores do sistema, e factores organizacionais. Estes autores apresentam uma visão interessante sobre a influência que uma condição técnica pode exercer numa vulnerabilidade, mas igualmente que essa vulnerabilidade também é influenciada pela competência que a força de trabalho tem na avaliação da condição, nomeadamente, nos esforços de inspecção e manutenção do operador, os quais, por sua vez, são influenciados, por diversos factores organizacionais, mas também por factores externos, o que permitiu fazer um paralelismo de reflexão interessante.

A obra de Chopra e Chaudhary (2020) revelou-se interessante, não só pelo aumento de conhecimento sobre a ISO 27001, como pela criação de um novo olhar sobre a melhoria contínua da segurança da informação em função da dinâmica do avanço tecnológico.

Boritz *et al*. (2019) evidenciou-se como relevante, pela sua abordagem sobre a integridade da informação e *framework*.

Kim e Solomon (2018) explicam os princípios fundamentais da segurança da informação, concentra-se em novos riscos, ameaças, e vulnerabilidades associadas à transformação para um mundo digital e ligado em rede.

Susanto e Almunawar (2018) não só apresenta uma vasta revisão bibliográfica, apresenta um conjunto de *frameworks*, e apresenta uma proposta de estrutura com uma nova abordagem para mapear os controles de segurança em seis domínios: *Stakeholder; Tool and Technology; Organization; Culture; Policy; Knowledge*. Para estes autores uma organização com um sistema de gestão de segurança da informação, pode demonstrar aos parceiros e aos clientes que identificou e mediu potenciais riscos de segurança e implementou uma política e controles de segurança que irá mitigar riscos. No entanto, como explicam Susanto e Almunawar (2018), como a segurança da informação não é uma tarefa fácil, é crucial que as organizações desenvolvam uma estrutura apropriada para enfrentar e monitorizar os riscos sistematicamente.

A obra de Sinnett (2008) é interessante não só pelos casos de estudo apresentados, mas também pela reflexão sobre as lições aprendidas e referenciadas no quadro 5 do presente estudo. Aprender com os erros ou com os eventos ocorridos é crucial para evitar que tal acontecimento se repita.

O artigo de Flowerday e Solms (2005) aborda a problemática da integridade da informação em tempo real e a necessidade de desenvolver um sistema de controle interno, em conformidade com a estrutura projectada e o qual pode ser baseado em *framework* padrão. Esta

sobreposição de monitorização auxilia a gestão da segurança, mas também reforça a sua eficácia, o que tranquiliza quem tem a responsabilidade de garantir a segurança, mas também quem tem a responsabilidade de tomar decisões.

Relativamente ao contributo e recomendações do *National Institute of Standards and Technology* (NIST) e das *International Organization for Standardization* (ISO), ambas as organizações representam pilares indissociáveis numa abordagem da problemática em estudo.

Quadro 6 – Autores de referência para a elaboração do Questionário

Autores	Título
Saffady (2021)	Managing Information Risks: Threats, Vulnerabilities, and Responses
Sperstad et al. (2020)	A comprehensive framework for vulnerability analysis of extraordinary events in power systems
Chopra & Chaudhary (2020)	Implementing an Information Security Management System. Security Management Based on ISO 27001 Guidelines
Boritz et al. (2019)	A Framework for Information Integrity Controls
Kim e Solomon (2018)	Fundamentals of information systems security
Susanto & Almunawar (2018)	Information Security Management Systems. A Novel Framework and Software as a Tool for Compliance with Information Security Standards.
Sinnett (2008)	The IIC's Excellence in Information Integrity Award
Flowerday & Solms (2005)	Real-time information integrity=system integrity+data integrity+continuous assurances

Fonte: Elaboração Própria

Dada a complexidade e amplitude do tema, optou-se por criar dois domínios de análise: interno e externo. No domínio externo, pretende-se conhecer como é efectuada a comunicação com o exterior. No domínio interno, o foco é o ciclo da informação dentro da própria organização, assim como, a existência ou não de procedimentos passíveis de promover e garantir a segurança e integridade dos dados e da informação. Para cada um dos domínios e subdomínios foram seleccionadas as questões consideradas mais pertinentes na óptica da integridade, e por inerência da segurança, seguindo a lógica da *Framework Core* - Identificar, Proteger, Detectar, Responder e Recuperar, Version 1.1 do *National Institute of Standards and Technology* (NIST, 2018).

Sendo uma adaptação na função identificar, não se pretende saber o que é que precisa ser protegido, mas sim identificar vulnerabilidades pelo que o objectivo é compreender como a informação é trocada e partilhada com o exterior, bem como é recolhida e tratada no interior.

A função proteger visa as políticas, procedimentos e controles envolvidos, pelo que se pretende conhecer os procedimentos implementados e as formas de avaliação de risco.

A função detectar permite a descoberta oportuna de ocorrências de segurança, pelo que é crucial analisar procedimentos de partilha, de atribuição de acessos e sua monitorização.

A função responder suporta a capacidade de conter o impacto de um possível incidente de segurança, neste sentido é essencial desenvolver intervenções que permitam conter, erradicar e notificar de preferência em tempo real.

A função recuperar, implica soluções, pelo que a finalidade é desenvolver e implementar actividades apropriadas para manter planos de resiliência e restaurar quaisquer recursos ou serviços que possam ter sido prejudicados, danificados ou eliminados devido a um incidente de segurança.

Para uma melhor compreensão no quadro 7, apresenta-se as áreas que se pretende analisar por domínio e subdomínio, com as funções, como ferramenta de reflexão para a formulação das questões.

Quadro 7 - Domínios e subdomínios de suporte à elaboração do questionário

Domínio – Envolvente Externa		
Subdomínios	Função	Descrição
Comunicações com o Exterior	**Identificar** – Compreender como a informação é trocada e partilhada com o exterior.	Via VPN, via proxy, túneis encriptados.
Monitorização de acesso à estrutura TI	**Proteger** – Verificar processos de segurança	Via sistema de IPS (intrusion prevention system) e sistema de IDS (intrusion detection system)
Domínio – Envolvente Interna		
Subdomínios	Função	Descrição
Recolha e Tratamento	**Identificar** - Compreender o contexto de negócio e os activos de informação.	Conhecer o enquadramento da gestão da informação.
Armazenamento, Backups e Destruição	**Proteger** – Verificar processos de segurança	Conhecer os procedimentos de segurança e avaliação de risco.

Controlo de Acessos, Comunicação Interna e Acesso Remoto	**Detectar** – Verificar possíveis eventos e falhas de segurança.	Analisar procedimentos de partilha, de atribuição de acessos e a sua monitorização.
Monitorização do uso do sistema	**Responder** – Mitigação e Melhoria	Analisar a utilização ferramentas de gestão de vulnerabilidades (scanners, testes e alertas de invasão).
Incidentes	**Recuperar –** Soluções	Conhecer os incidentes, retirar lições, restaurar e reduzir impacto.

Fonte: Elaboração Própria

De acordo com Hill e Hill (2008) para a elaboração do questionário, a opção recaiu sobre a concepção de perguntas fechadas e sempre que adequado com recurso a escala de *Likert*, para ampliar as possibilidades de resposta. Na formulação das questões foi tida em consideração a necessidade da sua objectividade, imparcialidade e clareza. Foram evitadas longas listas de opções de resposta e não foi estabelecida nenhuma hierarquia de importância na elaboração da estrutura. Foi desenvolvido um primeiro questionário e utilizado como caso piloto, para aferir a clareza e coerência das questões (Hill & Hill, 2008). Através da aplicação deste questionário obtiveram-se 18 respostas, com os respectivos comentários, questão a questão, os quais foram tidos em consideração na versão final do questionário a aplicar. De acordo com as recomendações foi incluída a opção *Não responde* na questão 1 sobre o género e na questão 27 a escala de Likert, foi alterada para *Nunca ou Raramente, Todos os dias, Uma a duas vezes por semana, Todas as semanas* e *Todos os meses*. Relativamente aos cargos por recomendação, optou-se por manter como questão aberta, apesar das dificuldades acrescidas do seu tratamento estatístico. Foi unanime a clareza das questões e a sua coerência. Ambos os questionários foram elaborados em plataforma online *(Google Forms)* e disponibilizado um *link* para preenchimento, em conformidade com os critérios definidos no estudo piloto e na construção da amostra. A disponibilização do *link* foi acompanhada com a devida explicação sobre o propósito do estudo. No caso do estudo piloto, o mesmo foi aplicado a dezoito profissionais inquiridos cujo perfil se apresenta na tabela 1.

Tabela 1 - Caracterização dos inquiridos no teste piloto

Variáveis	Categorias	N	%
Escalão Etário	18 a 30	8	44,44
	31 a 40	5	27,78
	41 a 50	4	22,22
	51 a 60	1	5,56
	Mais de 60	0	0,0
	Total	**18**	**100**
Género	Masculino	13	72,22
	Feminino	5	27,78
	Total	**18**	**100**
	Ensino Básico	0	0,0

Habilitações	Ensino Secundário	0	0,0
	Ensino Profissional	2	11,11
	Licenciatura	3	16,67
	Mestrado ou Doutoramento	13	72,22
	Total	**18**	**100**
Actividade Principal da Empresa	Agricultura, produção animal, caça, silvicultura e pesca	0	0,0
	Indústrias extractivas	1	5,56
	Indústrias transformadoras	0	0,0
	Electricidade, gás e água	0	0,0
	Construção	0	0,0
	Comércio por grosso e a retalho	3	16,67
	Transporte e armazenagem	1	5,56
	Alojamento, restauração e similares	0	0,0
	Actividades financeiras e de seguros	5	27,78
	Actividades imobiliárias	0	0,0
	Educação	2	11,11
	Actividades de saúde humana e apoio social	0	0,0
	Outros Sectores	6	33,33
	Total	**18**	**100**
Função/Cargo	Account Manager	2	11,11
	Business Analyst	2	11,11
	Security Engineer	3	16,67
	Project Manager	2	11,11
	Gestora clientes	2	11,11
	Marketing	2	11,11
	Docente e Investigação	2	11,11
	Gerente/ Chefe de Departamento	2	11,11
	Engenheiro	1	5,56
	Total	**18**	**100**
Antiguidade na Empresa	Menos de 1 ano	5	27,78
	Entre 1 - 5 anos	7	38,89
	Entre 6 – 9 anos	0	0,0
	Entre 10 - 20 anos	5	27,78
	Entre 21 - 30 anos	1	5,56
	Mais de 30 anos	0	0,0
	Total	**18**	**100**

3.4 População e Amostra

Para concretizar o propósito de desenvolvimento de uma *framework* de análise das vulnerabilidades de um sistema de informação, foi elaborado um inquérito por questionário dirigido a população empregada em território português, cuja actividade implicasse a utilização de equipamentos informáticos fixos e/ ou móveis, com o objectivo de identificar potenciais ameaças e mitigar riscos. Neste sentido, foi apurado através do Portal Pordata que a população empregada em 2020 em Portugal era de 4.814,1 milhares de indivíduos, distribuídos pelas profissões apresentadas no quadro 8.

Quadro 8 - População empregada: total e por profissões em 2020

Profissões	Nº Indivíduos
Profissões das forças armadas	21,2

Representantes do poder legislativo e órgãos executivos, dirigentes, directores e gestores executivos		280,1
Especialistas das actividades intelectuais e científicas		1.061,3
Técnicos e profissões de nível intermédio		529,5
Pessoal administrativo		415,1
Trabalhadores dos serviços pessoais, de protecção e segurança e vendedores		906,1
Agricultores e trabalhadores qualificados da agricultura, da pesca e da floresta		241,3
Trabalhadores qualificados da indústria, construção e artífices		590,6
Operadores de instalações e máquinas e trabalhadores da montagem		381,4
Trabalhadores não qualificados		387,5
	Total	**4.814,1**

Fonte: Pordata (2020)

Tendo em consideração que se considera como população, para determinação do tamanho de uma amostra, um conjunto de indivíduos que compartilham, pelo menos, uma característica comum e que como critério foi estabelecida a utilização no desempenho da actividade profissional de equipamentos informáticos fixos e/ ou móveis, foram excluídos os trabalhadores não qualificados e os operadores de instalações e máquinas e trabalhadores da montagem. Foram ainda excluídas todas as profissões das forças armadas, em virtude de as mesmas não poderem participar neste tipo de estudos sem autorização de hierarquias superiores, o que poderia em termos operacionais comprometer a recolha de informação pela espera na obtenção de autorizações. Por conseguinte, a população alvo foi constituída por 4.017,9 milhares de indivíduos. Relativamente ao cálculo do tamanho da amostra optou-se por uma margem de erro de 5% e um nível de confiança de 95%, tendo sido obtido o valor de 385 indivíduos pela aplicação da fórmula gaussiana, em que n = representa o tamanho da amostra que queremos calcular; N= representa o tamanho do Universo; Z = é o desvio do valor médio que nós aceitamos para alcançar o nível de confiança pretendido o que para 95% corresponde a Z=1,96, e = margem de erro máxima que se pretende admitir e p = a proporção que se espera encontrar.

$$n = \frac{N.Z^2.p(1-p)}{(N-1).e^2 + Z^2.p(1-p)}$$

A técnica de amostragem utilizada foi aleatória, tendo sido privilegiada como fonte principal de recolha de contactos as redes sociais, para solicitar a participação no estudo, em particular o LinkedIn e o Facebook.

Todos os dados foram tratados de forma agregada, salvaguardado o anonimato e a confidencialidade.

Capítulo 4 – Apresentação e interpretação dos resultados

Os dados foram recolhidos entre 23 de Junho de 2021 e 23 de Julho de 2021, via plataforma *Google Forms*, tendo sido recepcionados e validados 393, o que corresponde a um valor superior ao inicialmente calculado para amostra de 385 indivíduos, para um grau de confiança de 95% e uma margem de erro de 5%.

No que concerne à caracterização dos inquiridos o escalão etário mais frequente, é o de 31 a 40 anos, com 32,82%, o género masculino com 55,22% e em termos de habilitações a mais frequente é a licenciatura (tabela 2).

Tabela 2 - Caracterização sociodemográfica dos inquiridos

Variáveis	Categorias	N	%
Escalão Etário	18 a 30	121	30,79
	31 a 40	129	32,82
	41 a 50	105	26,72
	51 a 60	31	7,89
	Mais de 60	7	1,78
	Total	**393**	**100**
Género	Masculino	217	55,22
	Feminino	165	41,98
	Não Responde	11	2,80
	Total	**393**	**100**
Habilitações	Ensino Básico	14	3,56
	Ensino Secundário	63	16,03
	Ensino Profissional	57	14,50
	Licenciatura	189	48,09
	Mestrado ou Doutoramento	70	17,81
	Total	**393**	**100**

Relativamente à actividade principal da empresa onde o inquirido desempenha funções, com excepção de "outros sectores" a actividade mais frequente é o comércio por grosso e a retalho, relativamente às funções/ cargo o valor mais frequente corresponde à área de Serviço IT (40,71%). Sobre a antiguidade o escalão mais representativo é de 1 a 5, com 31,04%, logo seguido do escalão de 10 a 20 (29,26%) conforma ilustra a tabela 3.

Tabela 3 - Actividade principal da empresa e função/ cargo e antiguidade dos inquiridos

Variáveis	Categorias	N	%
Actividade Principal da Empresa	Agricultura, produção animal, caça, silvicultura e pesca	1	0,25
	Indústrias extractivas	0	0,00
	Indústrias transformadoras	2	0,51
	Electricidade, gás e água	17	4,33
	Construção	6	1,53
	Comércio por grosso e a retalho	54	13,74
	Transporte e armazenagem	16	4,07
	Alojamento, restauração e similares	22	5,60
	Actividades financeiras e de seguros	34	8,65
	Actividades imobiliárias	2	0,51
	Educação	40	10,18
	Actividades de saúde humana e apoio social	21	5,34
	Outros Sectores	178	45,29
	Total	**393**	**100**
Função/Cargo	**Gestão e Consultoria**: (Actividades imobiliárias, Comércio por grosso e a retalho, Actividades financeiras e de seguros, Actividades de Consultoria, de Engenharia Arquitectura e de Contabilidade)	142	36,13
	Educação e actividades sociais: (Actividades de saúde humana e apoio social, Educação)	54	13,74
	Sector terciários / Serviços: (Transporte e armazenagem, Alojamento, restauração e similares, Electricidade, gás e água)	24	6,11
	Serviço especializado/ intensivo: (Agricultura, produção animal, caça, silvicultura e pesca, Indústrias extractivas, Indústrias transformadoras, Outros Sectores)	13	3,31
	Serviço IT – (Administrador de Sistemas, Analista de gestão de acessos, Analista Funcional SAP, Analista Segurança, Analista SOC, Consultor IT, DevOps, Engenheiro *Cloud*, Engenheiro de redes, Engenheiro de Software, IT Project Manager, Programador, *Pentester*, *webdesign*)	160	40,71
	Total	**393**	**100**
Antiguidade na Empresa	Menos de 1 ano	**42**	10,69
	Entre 1 - 5 anos	**122**	31,04
	Entre 6 – 9 anos	**67**	17,05
	Entre 10 - 20 anos	**115**	29,26
	Entre 21 - 30 anos	**34**	8,65
	Mais de 30 anos	**13**	3,31
	Total	**393**	**100**

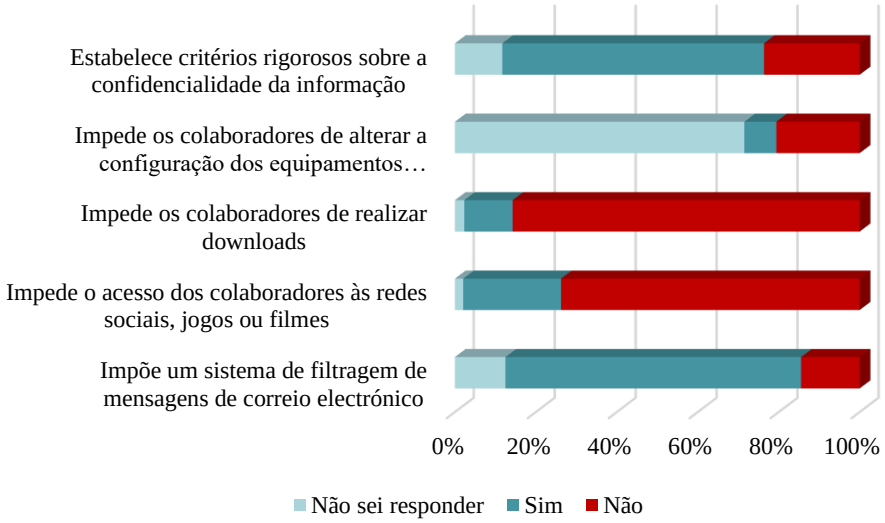
Sobre a política de segurança da informação e dos dispositivos (tabela 4) é interessante verificar que, apesar de 73,03% das empresas/ entidades imporem um sistema de filtragem de mensagens de correio electrónico, no entanto, não impedem o acesso dos colaboradores às redes sociais, jogos ou filmes (73,79%) nem de realizar *downloads* (85,75%). Ainda em termos de segurança o facto de apenas 7,89% dos inquiridos afirmar que não podem alterar a configuração dos equipamentos informáticos, configura uma preocupação em termos das políticas de segurança

em vigor nestas empresas/ entidades (tabela 4). Relativamente ao estabelecimento de critérios rigorosos sobre a confidencialidade da informação apenas 64,63% dos inquiridos reconhece a sua existência (tabela 4).

Tabela 4 - Política de segurança da informação e dos dispositivos

Questão 7 a 9 - No âmbito da política de segurança da informação e dos dispositivos, a sua empresa/ entidade:	Não sei responder %	Sim %	Não %
Impõe um sistema de filtragem de mensagens de correio electrónico	12,47	**73,03**	14,50
Impede o acesso dos colaboradores às redes sociais, jogos ou filmes	2,04	24,17	**73,79**
Impede os colaboradores de realizar downloads	2,29	11,96	**85,75**
Impede os colaboradores de alterar a configuração dos equipamentos informáticos	**71,50**	7,89	20,61
Estabelece critérios rigorosos sobre a confidencialidade da informação	11,70	**64,63**	23,66

Gráfico 1 - Política de segurança da informação e dos dispositivos



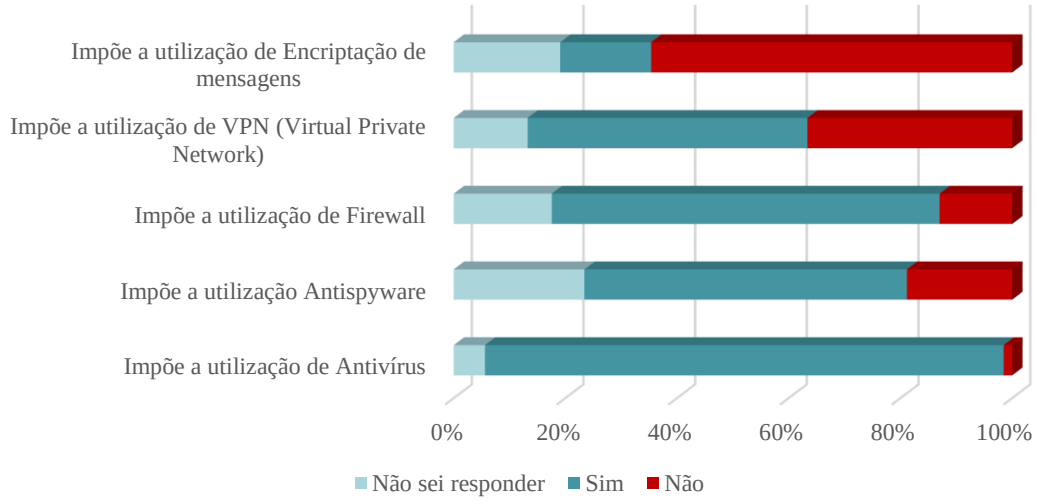
Em termos de ferramentas de protecção da informação e dos dispositivos, a utilização de antivírus é a mais frequente (92,88%). Apenas 69,47% utilizam firewall, e 57,76% *antispyware*, o que evidencia a necessidade de uma maior sensibilização sobre a importância de proteger estes activos (informação e dispositivos). Uma firewall analisa o tráfego da rede, e permite controlar os acessos evitando por um lado ataques, e por outro, que os funcionários tenham acesso a determinados conteúdos disponíveis pela internet, ou por exemplo às redes sociais em horário de trabalho. Apesar de alguns antivírus já incorporam detecção de spyware e adware, um *antispyware* específico, representa uma ferramenta de segurança importante, que não está a ser valorizada significativamente pelas empresas/ entidades alvo do estudo. O mesmo se aplica à utilização de VPN (*Virtual Private Network*). A utilização de VPN é uma solução prática e

simples que diminui consideravelmente o risco de falhas de segurança e é uma solução muito pertinente para o trabalho remoto, oferecendo uma ligação segura entre funcionários e o sistema interno, sem que seja rastreável por terceiros. A criptografia de e-mail é a ferramenta menos utilizada, e consiste em tornar ilegível o conteúdo das mensagens, de modo a impedir que informações potencialmente confidenciais sejam lidas por qualquer pessoa que não seja o destinatário. Apesar da sua fraca utilização (16,28%) curiosamente é a técnica mais antiga, e que hoje pode ser realizada de forma automática (tabela 5).

Tabela 5 - Ferramentas utilizadas para proteger a segurança da informação e dos dispositivos

Questão 12 – 16 Para proteger a segurança da informação e dos dispositivos, a sua empresa/ entidade:	Não sei responder %	Sim %	Não %
Impõe a utilização de Antivírus	5,60	**92,88**	1,53
Impõe a utilização *Antispyware*	23,41	**57,76**	18,83
Impõe a utilização de Firewall	17,56	**69,47**	12,98
Impõe a utilização de VPN *(Virtual Private Network)*	13,23	**50,13**	36,64
Impõe a utilização de Encriptação de mensagens	19,08	16,28	**64,63**

Gráfico 2 - Ferramentas utilizadas para proteger a segurança da informação e dos dispositivos

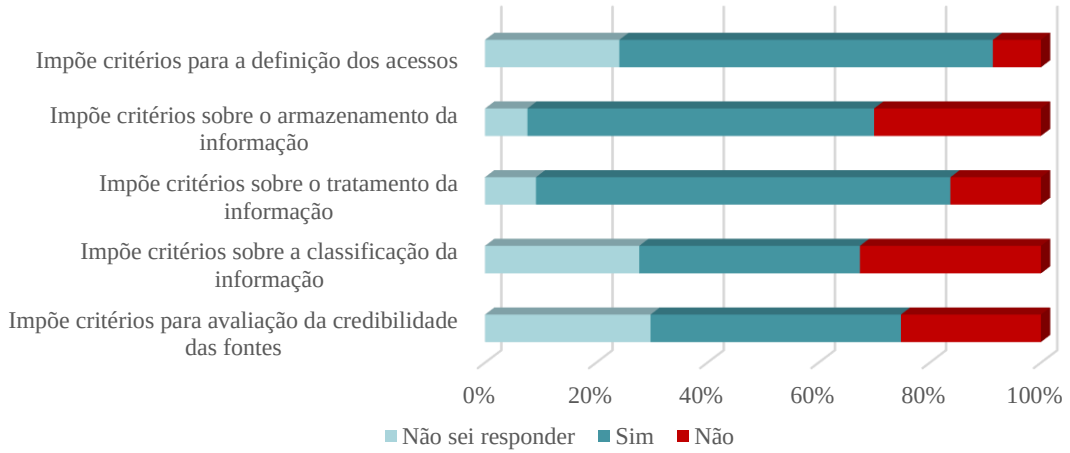


Como se apresenta na tabela 6, em termos de procedimentos a maior preocupação recai no tratamento da informação (74,55%), seguida da definição de acessos (67,34%) e do armazenamento (62,34%).

Tabela 6 – Procedimentos utilizados para proteger a segurança da informação e dos dispositivos

Questão 17- 21 - Para proteger a informação recolhida e a sua integridade, a sua empresa/ entidade:	Não sei responder %	Sim %	Não %
Impõe critérios para avaliação da credibilidade das fontes	29,77	**45,04**	25,19
Impõe critérios sobre a classificação da informação	27,74	**39,69**	32,57
Impõe critérios sobre o tratamento da informação	9,16	**74,55**	16,28
Impõe critérios sobre o armazenamento da informação	7,63	**62,34**	30,03
Impõe critérios para a definição dos acessos	24,17	**67,18**	8,65

Gráfico 3 - Procedimentos utilizados para proteger a segurança da informação e dos dispositivos

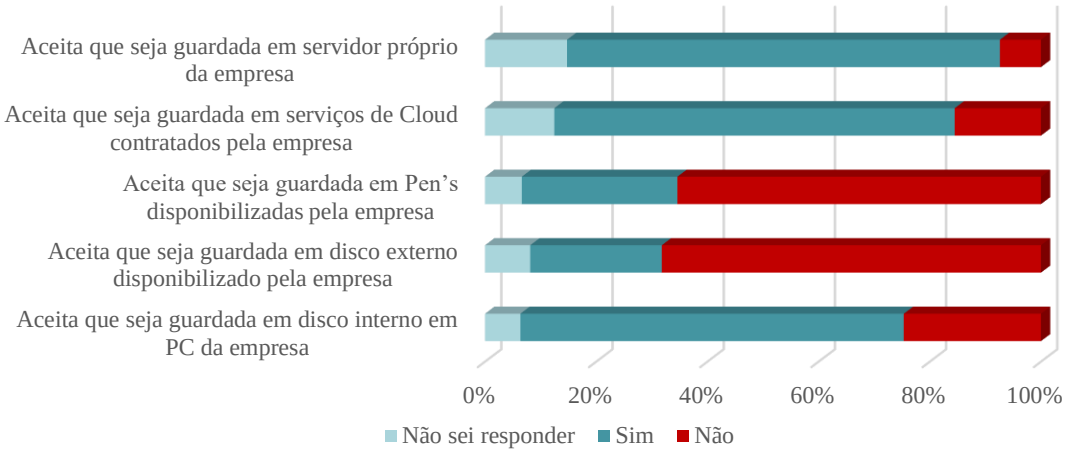


Relativamente ao armazenamento da informação, é interessante destacar a preocupação evidenciada pela da maioria das empresas em estudo (tabela 7) sobre a utilização de discos externos e *Pen's*, os quais não são permitidos, sendo apenas permitido guardar em disco interno de PC da empresa (68,96%), serviços de *Clould* contratados pela empresa (72,01%) e servidor próprio da empresa (77,86%).

Tabela 7 – Procedimentos para proteger a informação armazenada e a sua integridade

Questão 22 – 26 - Para proteger a informação armazenada e a sua integridade, a sua empresa/ entidade:	Não sei responder %	Sim %	Não %
Aceita que seja guardada em disco interno em PC da empresa	6,36	**68,96**	24,68
Aceita que seja guardada em disco externo disponibilizado pela empresa	8,14	23,66	**68,19**
Aceita que seja guardada em Pen's disponibilizadas pela empresa	6,62	27,99	**65,39**
Aceita que seja guardada em serviços de *Cloud* contratados pela empresa	12,47	**72,01**	15,52
Aceita que seja guardada em servidor próprio da empresa	14,76	**77,86**	7,38

Gráfico 4 - Procedimentos utilizados para proteger a segurança da informação e dos dispositivos

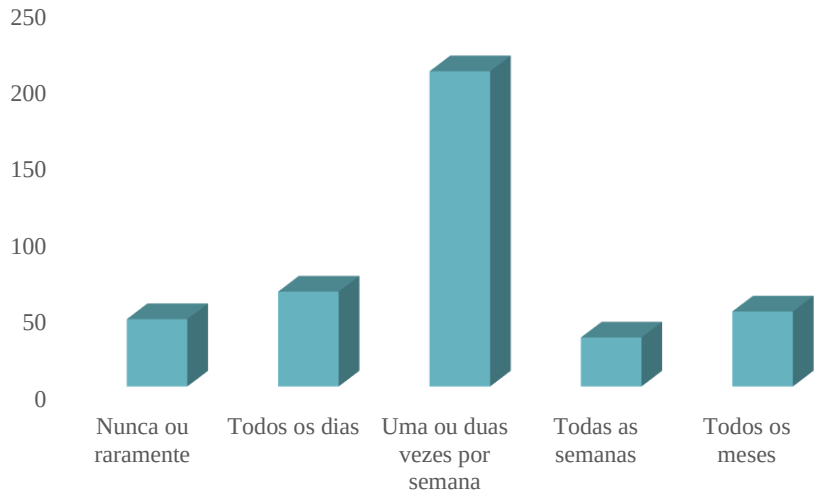


No que concerne à política de *backups* apenas 11,20% das empresas, não tem este procedimento como rotina, sendo a periodicidade mais recomendada pela maioria (52,42%) "Uma ou duas vezes por semana" (tabela 8).

Tabela 8 - Periodicidade recomendada pela empresa para a realização de backups

Questão 27 - Qual das seguintes afirmações caracterizam melhor a periodicidade recomendada pela empresa para a realização de backups	%
Nunca ou raramente	11,20
Todos os dias	15,78
Uma ou duas vezes por semana	52,42
Todas as semanas	8,14
Todos os meses	12,47

Gráfico 5 - Periodicidade recomendada pela empresa para a realização de backups

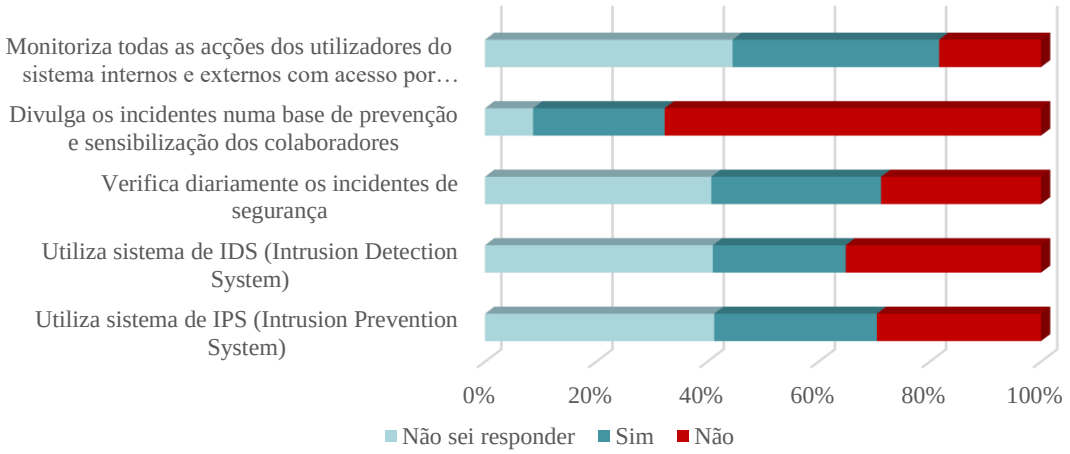


No que concerne aos procedimentos para monitorizar a utilização do sistema e as ameaças sofridas (questões 28-32), os resultados obtidos evidenciam uma maturidade em termos de tecnologia de controles de segurança, no entanto, existe pouca informação sobre o que se passa em termos de incidentes, com 76,33% a afirmarem que não são informados dos incidentes ou que não têm acesso aos relatórios de segurança. A baixa divulgação dos incidentes atrasa a mudança de comportamentos. Como evidenciam os dados, as soluções de segurança maioritariamente não são divulgadas numa base de prevenção e sensibilização dos colaboradores e 44,53% dos inquiridos desconhece se o sistema é monitorado e com que soluções. Em síntese, podemos assumir uma maturidade relativa a soluções de segurança de informação sendo que apenas 15,27% sofreu um ataque que resultou em perdas para a empresa (tabela 9).

Tabela 9 – Procedimentos para monitorizar a utilização do sistema e as ameaças sofridas

Questão 28 – 32 - Para monitorizar a utilização do sistema e as ameaças sofridas, a sua empresa/ entidade:	Não sei responder %	Sim %	Não %
Utiliza sistema de IPS (*Intrusion Prevention System*)	41,22	29,26	29,52
Utiliza sistema de IDS (*Intrusion Detection System*)	40,97	23,92	35,11
Verifica diariamente os incidentes de segurança	40,71	30,53	28,75
Divulga os incidentes numa base de prevenção e sensibilização dos colaboradores	8,65	23,66	67,68
Monitoriza todas as acções dos utilizadores do sistema internos e externos com acesso por login	44,53	37,15	18,32

Gráfico 6 - Procedimentos para monitorizar a utilização do sistema e as ameaças sofridas



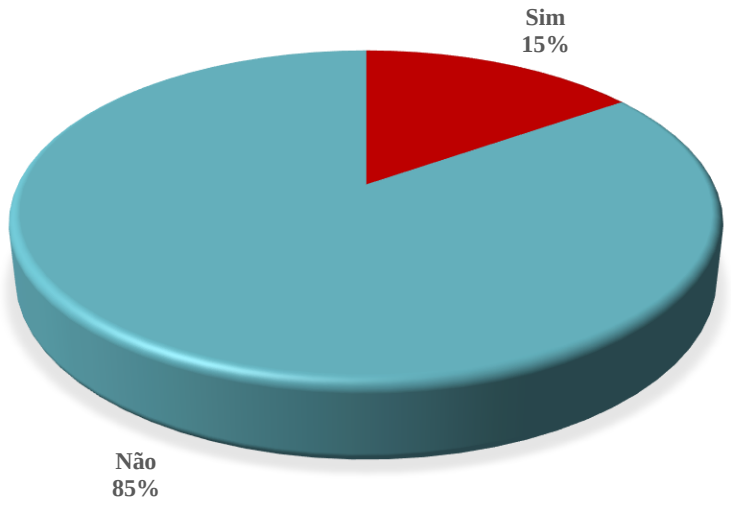
A transição para o trabalho remoto, na sequência das medidas de combate à pandemia veio expor muitas empresas a um aumento das suas vulnerabilidades, gerando um terreno propício para o crescimento do número de ataques. É importante destacar que, das empresas que foram alvo de ataque ou acesso indevido com perda de informação ou horas de trabalho, com excepção

da classificação “Outros sectores” como actividade principal, as “Actividades financeiras e de seguros” foram as mais representativas (16,66%) (tabela 10).

Tabela 10 - Nos últimos seis meses sofreu algum ataque informático ou acesso indevido resultando na perda de informação ou de horas de trabalho?

Questão 33 - Nos últimos seis meses sofreu algum ataque informático ou acesso indevido resultando na perda de informação ou de horas de trabalho?	%
Sim	15,27
Não	84,73

Gráfico 7 - Nos últimos seis meses sofreu algum ataque informático ou acesso indevido, resultando na perda de informação ou de horas de trabalho?

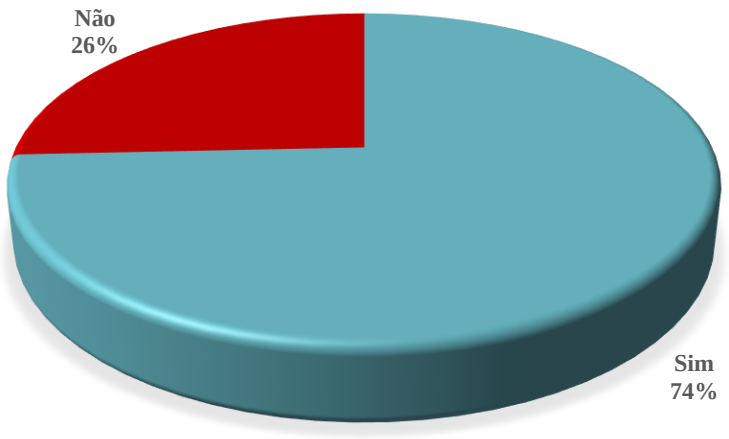


A observação da tabela 11, revela outro aspecto relevante é que cerca de 26% dos inquiridos desconhece qual o procedimento a seguir em caso de violação do seu acesso, de vírus ou ataque informático.

Tabela 11 - Em caso de uma violação do seu acesso, um vírus ou um ataque informático sabe o procedimento a seguir?

Questão 14 - Em caso de uma violação do seu acesso, um vírus ou um ataque informático sabe o procedimento a seguir?	%
Sim	74,30
Não	25,70

Gráfico 8 - Em caso de uma violação do seu acesso, um vírus ou um ataque informático sabe o procedimento a seguir?

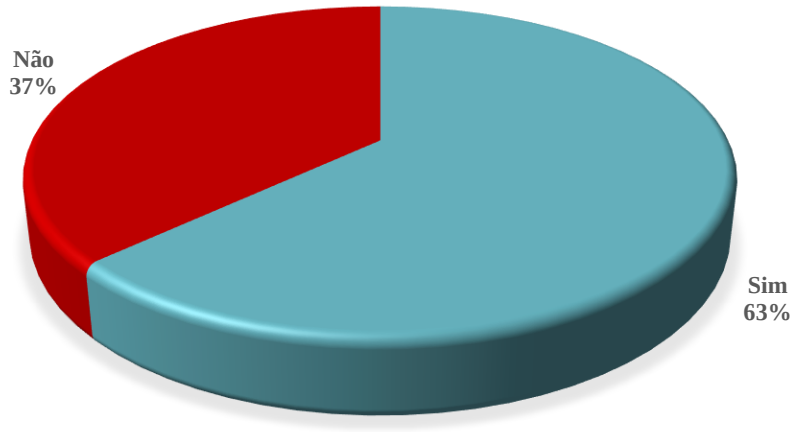


Sobre o grau de conhecimento da estrutura de elementos responsáveis pela segurança da informação da empresa, 63,10% afirma que sim, o que evidencia que a existência de uma relação directa com os elementos responsáveis pela segurança. A divulgação de informação e de recomendações ajuda a envolver toda a empresa no processo de assegurar a segurança da informação, pelo que é positivo dar a conhecer os seus responsáveis directos e as equipas que compõem (tabela 12).

Tabela 12 - Conhece a estrutura de elementos responsáveis pela segurança da informação da empresa?

Questão 35 - Conhece a estrutura de elementos responsáveis pela segurança da informação da empresa?	%
Sim	63,10
Não	36,90

Gráfico 9 - Conhece a estrutura de elementos responsáveis pela segurança da informação da empresa?

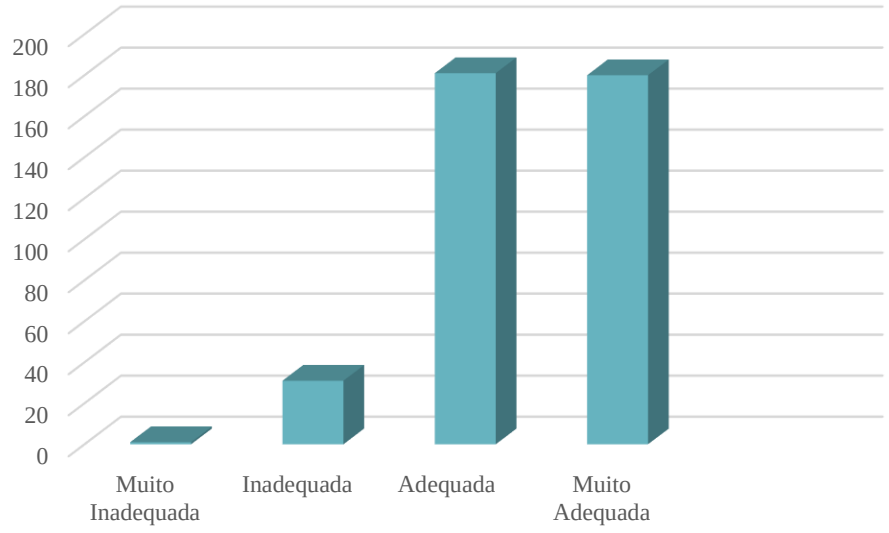


Relativamente à política de segurança somente 8,14% a considera como Inadequada ou Muito Inadequada (tabela 13).

Tabela 13 - Como classifica a política de segurança da informação em vigor na empresa?

Questão 36 - Como classifica a política de segurança da informação em vigor na empresa?	%
Muito Inadequada	0,25
Inadequada	7,89
Adequada	46,06
Muito Adequada	45,80

Gráfico 10 - Como classifica a política de segurança da informação em vigor na empresa?

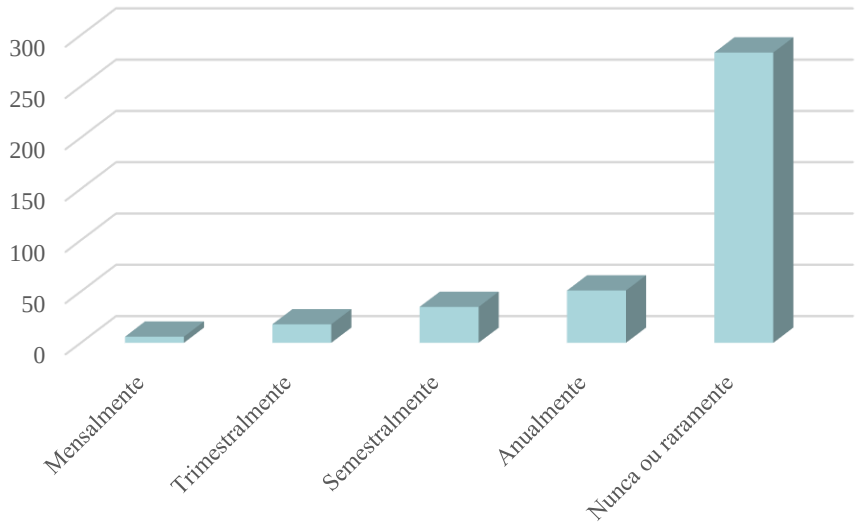


As ameaças à segurança da informação têm diferentes origens e estão em constante evolução, o que implica uma atitude proactiva de permanente reflexão e adaptação das medidas de segurança. Esta dinâmica reforça a pertinência e utilidade das acções de formação. No entanto, para 72,01% dos inquiridos "Nunca ou raramente" são realizadas (tabela 14).

Tabela 14 - Com que frequência são realizadas formações sobre segurança da informação?

Questão 37 - Com que frequência são realizadas formações sobre segurança da informação?	%
Mensalmente	1,53
Trimestralmente	4,58
Semestralmente	8,91
Anualmente	12,98
Nunca ou raramente	72,01

Gráfico 11 - Com que frequência são realizadas formações sobre segurança da informação?

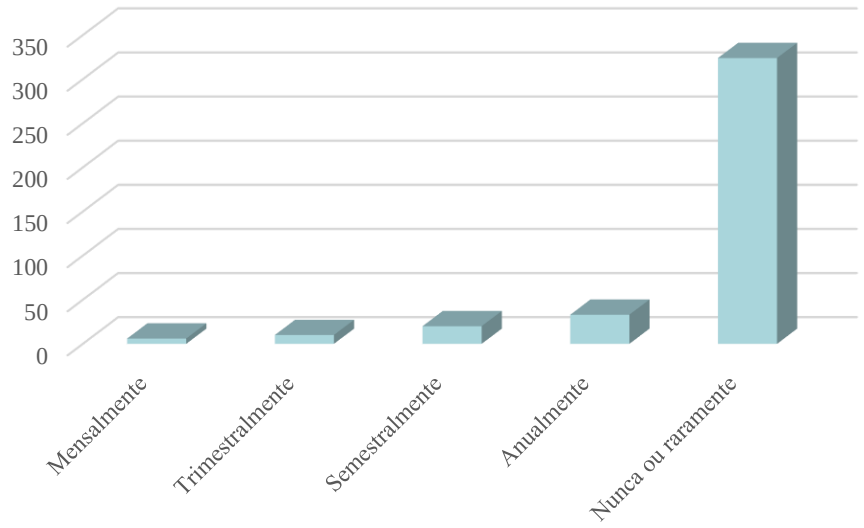


Em conformidade com os resultados obtidos na questão anterior, segundo 82,44% dos inquiridos "Nunca ou raramente" são realizadas acções de formação baseadas em acidentes ocorridos (tabela 15). Esta constatação é muito relevante, tendo em consideração que muitos dos incidentes de segurança têm origem num erro ou desconhecimento de um colaborador e neste sentido, as acções de formação constituem uma base essencial para a adopção de boas práticas no acesso, tratamento, utilização e armazenamento da informação.

Tabela 15 - Com que frequência são feitas acções de formação baseados em incidentes acontecidos?

Questão 38-Com que frequência são feitas acções de formação baseados em incidentes acontecidos?	%
Mensalmente	1,53
Trimestralmente	2,54
Semestralmente	5,09
Anualmente	8,40
Nunca ou raramente	82,44

Gráfico 12 - Com que frequência são feitas acções de formação baseados em incidentes acontecidos?

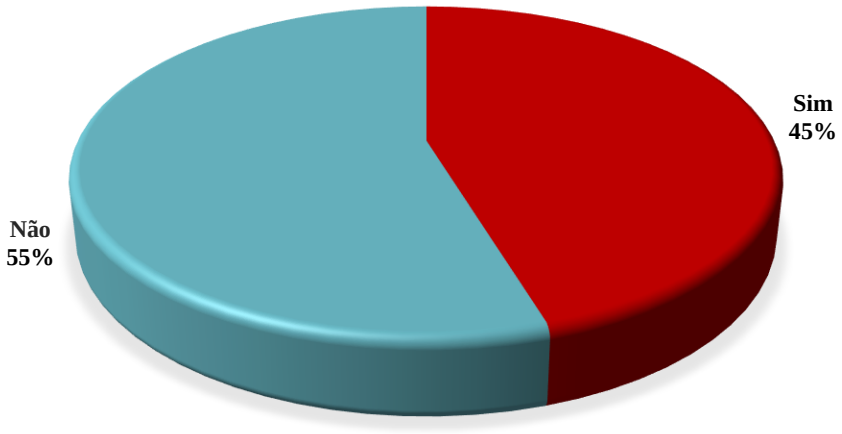


Na tabela 16 é possível observar que apesar da maioria dos inquiridos não considerarem que têm necessidades de formação 45,29%, adopta uma posição divergente. É importante salientar que 40,71% dos inquiridos exercem função/cargo na área de IT. Perante esta realidade é plausível afirmar que existe um maior investimento em soluções do que na formação e mudança de comportamentos.

Tabela 16 - Considera que tem necessidade de formação na área da segurança da informação?

Questão 39 - Considera que tem necessidade de formação na área da segurança da informação?	%
Sim	45,29%
Não	54,71%

Gráfico 13 - Considera que tem necessidade de formação na área da segurança da informação?



Em relação à Questão 20 - *Como classifica o seu comportamento no âmbito da segurança e protecção da informação da empresa?* o valor médio obtido é de 4,08%, com a maioria dos inquiridos a definirem o seu comportamento como prudente e muito prudente

Tabela 17 - Como classifica o seu comportamento no âmbito da segurança e protecção da informação da empresa?

Questão 40 - Como classifica o seu comportamento no âmbito da segurança e protecção da informação da empresa?	%
1 – Nada prudente	0,00
2	1,78
3	25,19
4	36,13
5 – Muito prudente	36,90

Capítulo 5 - *Framework* de análise das vulnerabilidades

A *framework* tem como base uma infraestrutura, em que apenas pessoas autorizadas (confidencialidade) têm acesso aos recursos e informação completa e livre de erros (integridade) e que a mesma esteja acessível sempre que necessária (disponibilidade). Optou-se por uma infraestrutura *Cloud*, onde a segurança é pensada "by design", permitindo a sua escalabilidade, gestão centralizada e com controlos de acesso a todo ciclo de vida da informação. Este modelo não está restrito a computadores e utilizadores, podendo ser implementado para dispositivos moveis, IoT e futuros dispositivos que necessitem de dados e ou informação para cumprir uma função. Optou-se pela plataforma *Cloud Azure* por suportar na sua totalidade esta *framework* seja na sua concepção de segurança "by design" como a possibilidade de alterar e ajustar a qualquer área de negócio. Recomenda-se ter uma subscrição *Premium* para tirar total partido desta *framework*.

Figura 3 - Modelo de Conceptual

Quadro 9 - *Framework* de análise das vulnerabilidades por domínio da Envolvente Externa

Domínio – Envolvente Externa				
Subdomínio 1 – Comunicações com o Exterior				
Identificar	Proteger	Detectar falhas	Responder	Recuperar/ Solução
Correio electrónico	Impor um sistema de filtragem de mensagens de correio electrónico.	Analisar comportamentos e a sua conformidade com a política de segurança. Verificação em *Cloud* de ficheiros recebidos/ enviados para validação da sua integridade em ambiente seguro.	Antivírus; *Antispyware; Firewall*; *AntiSpam*; estabelecer critérios para a utilização dos canais de comunicação com o exterior e encriptação de mensagens. Verificar a reputação do domínio. Actualizar base de dados de SPAM para bloqueio automático.	Formação sobre procedimentos de segurança da informação. Divulgação de incidentes detectados e o plano de mitigação. Treino com base em incidentes ocorridos.
Redes sociais, plataformas de jogos, música, filmes, etc.	Impedir o acesso dos colaboradores não autorizados às redes sociais, jogos ou filmes. Impedir a divulgação de informação confidencial. Impedir a partilha de ficheiros e ou informação da empresa via redes sociais.	Monitorização de acessos e actividades. Monitorizar o acesso a documentos internos e a sua partilha por canais não autorizados. Monitorizar tentativas de acesso a documentos confidenciais.	Estabelecimento de critérios de utilização de forma a evitar exposição a riscos de acesso indevido a informação. Bloqueio de partilha de documentos fora dos canais e serviços autorizados. Monitorização de acessos assim como informação consultados e ou alterada.	Impedir os colaboradores de alterar a configuração dos equipamentos informáticos. Impedir o acesso a documentos não autorizados. Revogação de acessos aos serviços partilhados, assim como o acesso a informação restrita. Aplicar políticas de acesso granular. Histórico de acessos para mitigar e ou responder a acesso indevido a informação.
Subdomínio 2 – Monitorização de acesso à estrutura TI				
Controlo de acesso	Acesso por identificação com password, impressão digital ou biometria.	Alerta de tentativa de acesso de utilizador não autorizado. Alertas para pedidos de alteração de password.	Gestão centralizada de utilizadores. Gestão centralizada de políticas de segurança para o domínio e por grupo de utilizadores. Acessos temporários com permissões limitadas.	Registo da workstation no *Azure AD services*, habilitando o *multi-factor authentication*, Gestão de acessos centralizada e com permissões granulares de acesso.

Quadro 10 - *Framework* de análise das vulnerabilidades por domínio da Envolvente Interna

Domínio – Envolvente Interna			
Subdomínio 1 – Recolha e Tratamento			
Identificar	Detectar falhas	Proteger/Responder	Recuperar/ Solução/ Resultados esperados
Dados e Informação	Vulnerabilidades nos controles de acesso. Armazenamento de dados e informação em sistemas de gestão de base de dados desactualizados. Acesso por fontes não auditadas aos dados. Sistema operativo, aplicações, dispositivos com acesso aos dados e informação desactualizados. Partilha de dados com terceiros, que, não estão sujeitos aos mesmos critérios e normas de segurança.	Utilizar sistemas de gestão de bases de dados em *Cloud*. Aplicar criptografia assimétrica para acesso a base de dados. Transito de dados devem ser encriptados *end-to-end*. Dados armazenado devem estar encriptados. SGBD integrado com SIEM e SOAR.	Responsabilidade partilhada na *Cloud* (Paas / SaaS). SGBD actualizado com as correcções de segurança automaticamente. Acessos granulados e restritos ao utilizador e/ ou aplicações que requerem acesso. Alta disponibilidade e redundância dos dados.
Subdomínio 2 – Armazenamento, *Backups* e Destruição			
Armazenamento e *Backup*	Dispositivos de armazenamento físicos sem encriptação. Acesso aos dispositivos/ serviços de armazenamento sem restrições. *Backup* sem encriptação. Ficheiros de *backup* com informação sensível sem controlo de acesso. *Backup* com ponto único de falha.	Utilização de um sistema de *backup* em nuvem como o *Azure Backup*. *Backup* encriptados. Controle de acesso aos *Backup*. Gestão centralizada.	Gestão centralizada. Cópias de segurança de máquinas virtuais, servidores, serviços de base de dados, serviços SAP em escala. Cópias de segurança com redundância local, geo-redundante e com redundância entre zonas. Alta disponibilidade dos dados.
Destruição	Copias não autorizadas de dados/ informação/ ficheiros. Destruição parcial de dados. Permanência de dados em *backups* anteriores. Informação a ser destruída alojada em dispositivos/ serviços não estriáveis e sem controlos de acesso.	Gestão centralizada de ficheiros. Políticas para destruição de dados aplicada a toda infraestrutura (utilizadores/ dispositivos móveis) Utilização do *Azure Custumer Data Protection.* Utilização do *Azure Data Protection*.	Gestão centralizada das políticas de destruição e recuperação de ficheiros/arquivos. *Compliance* com RGPD. Possibilidade de recuperação.
Subdomínio 3 – Controlo de Acessos, Comunicação Interna e Acesso Remoto			
Acesso remoto	Utilização de contas comunitárias. Roubo de Password. Perda/ Roubo equipamento.	Substituição de Password por certificados digitais. Utilização de uma plataforma *Bastion/ Jumpbox* para acesso aos servidores. Acessos restritos e com privilégios limitados. Sistema de gestão automática de certificados.	Utilização de criptografia assimétrica. Não exposição dos IP´s públicos dos servidores. Auto-renovação das chaves pública e privada. Mitiga a tentativa de intrusão e *zero-days exploits.*
Subdomínio 4 – Monitorização do uso do sistema			
Users	Monitorizar com base em heurística. Monitorizar os acessos a aplicações internas. Monitorizar o acesso a documentos internos assim como a sua partilha interna/ externamente.	Definição de políticas de segurança centralizadas. Utilização de Proxys para registo de actividade na Web. Registo centralizado para analise em tempo real e correlação de eventos. Utilização de solução SIEM. Utilização do *Microsoft Sentinel*.	Recolher dados à escala da nuvem em todos os utilizadores, dispositivos, aplicações e infra-estruturas, tanto no local como em múltiplas nuvens. Resposta rápida a incidentes. Registo centralizado de todas as actividades.
Serviços	Acessos indevidos. Acessos não autorizados.	Utilização de solução SIEM. Utilização do	Resposta rápida a incidentes com

	Incompatibilidade de software. Alteração dos parâmetros de monitorização. Funcionamento incorrecto de produto.	*Microsoft Sentinel*. Utilização de SOAR para uma resposta rápida e automatizada.	orquestração integrada e automatização de tarefas. Investiga ameaças com o uso de inteligência artificial, e procura por actividades suspeitas em escala. Monitorização centralizada de toda infra-estrutura. Partilha de informação entre os elementos de rede e o SIEM encriptado.
Subdomínio 5 – Incidentes			
Detecção de intrusão por ataque	Ataques maliciosos de fontes anónimas. Exploração de vulnerabilidades de software. Exploração de vulnerabilidades de sistema operativo. *Zero-days exploitaion.*	Suite de segurança de nova geração: *Anti-virus, anti-spyware, Next-generation Firewall*, Anti-SPAM, software para DLP e políticas de segurança ajustadas ao negócio.	As suites de nova geração para além de reagirem a vulnerabilidades conhecidas, devido a integração com inteligência artificial, permite por heurística prevenir de forma mais eficaz ataques conhecidos e desconhecidos.
Fraquezas do sistema	Sistema operativo desactualizado. Fim de vida do produto. Correcções de segurança não aplicadas. Acesso físico a infraestrutura sem controlo de acesso. Controles de acesso vulneráveis. Utilização de software com suporte descontinuado. Utilização de software pirata.	Actualização dos sistemas operativos, aplicações, bases de dados e *firmware* dos dispositivos. Aplicação de correcções de segurança fornecidas pelos proprietários dos produtos. Rever as políticas de segurança e comparar as melhores práticas recomendada pelos fornecedores de produto/ serviço. Gestão centralizada de licenças e de suporte de produto.	Correcções de segurança aplicadas. Melhor desempenho. Permite uma maturidade de segurança para minimizar os danos em caso de algum incidente de segurança bem-sucedido. A infraestrutura estará em conformidade com as melhores práticas.

Capítulo 6 - Conclusões e Recomendações

Como mencionado anteriormente, a segurança e integridade da informação não é um tema novo, no entanto, a evolução dos procedimentos e da tecnologia, no âmbito da recolha, tratamento e armazenamento da informação, de que são exemplos as técnicas de mineração, o recurso à inteligência artificial, ou a *Cloud*, têm contribuído para a construção de um novo olhar, que consiste não apenas em proteger a infraestrutura onde a informação é alojada, mas também, em proteger a informação em todo o seu ciclo de vida.

Neste contexto, a segurança da informação e a sua integridade, sendo parte de cibersegurança são um desafio quotidiano para as organizações, como se evidencia, quer na revisão bibliográfica, quer nos dados obtidos. Por conseguinte é importante destacar que existe um investimento primário em hardware e software e um baixo investimento nos colaboradores, no sentido de os preparar e dotar de conhecimentos e competências em conformidade com as boas práticas. Quanto maiores e melhores forem as competências, melhor será o desempenho em termos de comportamentos seguros online, o que aumenta a capacidade para enfrentar ameaças e reduz a exposição ao risco. Para o efeito, é crucial investir em formação e treino destinada aos colaboradores, como se evidenciou na análise aos resultados obtidos, bem como, apostar numa maior inclusão destes na política de segurança da informação da organização. Efectivamente, perante os novos paradigmas, e a rapidez com que tecnologia e conhecimento se tornam obsoletos, os colaboradores devem ser encarados na definição da política de segurança como beneficiários, mas também, como contribuintes. Este aspecto é muito importante, tendo em consideração que a maioria dos incidentes têm na sua origem comportamentos humanos, acidentais por desconhecimento ou negligencia, mas também intencionais, que é necessário acautelar e prevenir. Muitos destes comportamentos só podem ser detectados pela observação, análise e avaliação.

Assim, uma das linhas condutoras que alicerçou a elaboração da Framework foi criar uma ferramenta de gestão, que permita contribuir para essa análise e avaliação do envolvimento dos colaboradores, no esforço único para mitigar vulnerabilidades e antecipar incidentes relativos a segurança e integridade da informação. A opção por computação em nuvem justifica-se pelo facto de a mesma oferecer processos de segurança que estão de acordo com as melhores práticas.

Em trabalhos futuros, considera-se muito pertinente a criação de uma plataforma pública para partilha de incidentes de segurança e acções de mitigação. Aprender com os erros ou com incidentes ocorridos é determinante para evitar que tal acontecimento se repita. Outro aspecto, igualmente importante que é essencial ter presente é que a velocidade e dinâmica da evolução de ameaças no ciberespaço, impõe que exista informação em tempo real, ou com um desfasamento

temporal mínimo, sendo que a monitorização não só auxilia a gestão da segurança, como reforça a sua eficácia, o que tranquiliza quem tem a responsabilidade de garantir a segurança, mas também quem tem a responsabilidade de tomar decisões.

Bibliografia

Alhalafi, N., & Veeraraghavan, P. (2019). Privacy and Security Challenges and Solutions in IOT: A review. *International Conference on Smart Power & Internet Energy Systems.*, *322*, p. 012013. doi:10.1088/1755-1315/322/1/012013

Al-Mamary, Y. H., Shamsuddin, A., & Aziati , N. (2014). The Role of Different Types of Information Systems In Business Organizations: A Review. *International Journal of Research (IJR), 1*(7), pp. 1279-1286.

Augusto, A. (2014). Metodologias quantitativas/ metodologias qualitativas: mais do que uma questão de preferência. *Forum Sociológico Série II, 24*, pp. 1-9. doi:10.4000/sociologico.1073

Bapty, T., & al., e. (2017). *Handbook of System Safety and Security. Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems.* United States: Elsevier Inc.

Boeckl, K., & et al. (2021). *Considerações para Gerenciar Riscos de Privacidade e Segurança Cibernética na Internet das Coisas (IoT). NIST Interagency/Internal Report (NISTIR) - 8228pt.* Gaithersburg: National Institute of Standards and Technology (NIST).

Boritz, J. E., & et al. . (2019). *A Framework for Information Integrity Controls.* Canada: Chartered Professional Accountants of Canada (CPA Canada).

Brandão, P. R., & Rezende, M. (2020). Data: The most valuable commodity. *Kriativ.tech, 8*(1), pp. 1-7. doi:10.31112/kriativ-tech-2020-08-47

Cherdantseva, Y., & Hilton, J. (2013). A Reference Model of Information Assurance & Security. *Conference: Availability, Reliability and Security (ARES), 2013 Eighth International Conference on Project: Secure*BPMN* (pp. 546-555). Regensburg, Germany: IEEE. doi:10.1109/ARES.2013.72

Chopra, A., & Chaudhary, M. (2020). *Implementing an Information Security Management System. Security Management Based on ISO 27001 Guidelines.* New York: Springer Science+Business Media New York. doi:10.1007/978-1-4842-5413-4

Creswell, J. W. (2014). *Research design: qualitative, quantitative, and mixed methods approaches* (4th ed.). United States of America: SAGE Publications, Inc.

Dashti, S., Giorgini, P., & Paja, E. (2017). Information Security Risk Management. *10th Conference: IFIP Working Conference on The Practice of Enterprise Modeling* (pp. 18-33). Leuven, Belgium: Springer. doi:10.1007/978-3-319-70241-4_2

Flowerday, S., & Solms, R. (2005). Real-time information integrity=system integrity+data integrity+continuous assurances. *Computers & Security, 24*, pp. 604-613. doi:10.1016/j.cose.2005.08.004

Furnell, S. M., Katsikas, S., Lopez, J., Patel, A., & Editors. (2008). *Securing Information and Communications Systems. Principles, Technologies, an\ d Applications.* Norwood, United States of America: Artech House, Inc.

Griffor, E. (2017). *Handbook of System Safety and Security. Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems.* United States of America: Elsevier Inc.

House, N. (2017). *The Complete Cyber Security Course* (Vol. I). London: StationX Ltd.

Igried, A.-K., Al-Wahshat, H., Igried, B., & Takialddin, A.-S. (2019). Risk and Vulnerability Analyses for the protection of Information for Future communication security Based Neural Networks. *Journal of Advanced Sciences and Engineering Technologies, 2*(1), pp. 31-39. doi:10.32441/jaset.02.01.03

INFORMA. (2021). *Diretório de todas as empresas portuguesas*. Obtido em 26 de Maio de 2021, de Informa D&B Portugal: https://diretorio.informadb.pt/

Kim, D., & Solomon, M. (2018). *Fundamentals of information systems security* (3rd ed.). United States of America: Jones & Bartlett Learning.

Kure, H. I., Islam, S., & Razzaque, M. (2018). An Integrated Cyber Security Risk Management. Approach for a Cyber-Physical System. *Applied Sciences, 8*(898), pp. 1-29. doi:10.3390/app8060898

Laudon, K. C., & Laudon, J. (2018). *Management Information Systems. Managing the Digital Firm.* England: Pearson Education Limited.

Leavy, P. (2017). *Research Design. Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches.* New York: Guilford Publications, Inc.

Leeuw, K. M., & Bergstra, J. (2007). *The History of Information Security. A Comprehensive Handbook.* Netherlands: Elsevier B.V. doi:10.1016/B978-0-444-51608-4.X5000-7

Magalhães, M., & Hill, A. (2008). *Investigação por Questionário* (2ª ed.). Lisboa: Edições Sílabo.

Merkow, M. S., & Breithaupt, J. (2014). *Information Security: Principles and Practices.* United States of America: Pearson Education, Inc.

National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1.* USA: National Institute of Standards and Technology (NIST). doi:10.6028/NIST.CSWP.04162018

O'Brien, J. A., & Marakas, G. (2010). *Introduction to Information Systems* (15th ed.). New York: McGraw-Hill/Irwin.

Orvalho, L., Figueiredo, B., & Pinto, H. (2020). IoT e Internet 5G. *Kriativ.tech*, pp. 1-6. doi:10.31112/kriativ-tech-2018-01-22

Otero, A. R. (2019). *Information Technology Control and Audit* (5th ed.). Florida: Taylor & Francis Group, LLC.

Piteira, M., Aparicio, M., & Costa, C. (2019). A Ética na Inteligência Artificial: Desafios. *CISTI'2019 - 14ª Conferência Ibérica de Sistemas e Tecnologias de Informação* (pp. 1-6). Coimbra: AISTI - Associação Ibérica de Sistemas e Tecnologias de Informação.

Pordata. (2020). *População empregada: total e por profissões*. Obtido em 20 de Maio de 2021, de Emprego e Mercado de Trabalho: https://www.pordata.pt/Portugal/Popula%c3%a7%c3%a3o+empregada+total+e+por+profiss%c3%b5es-3385

Quivy, R., & Campenhoudt, L. (2018). *Manual de Investigação em Ciências Sociais.* Lisboa: Gradiva.

Rees, J., Bandyopadhyay, S., & Spafford, E. (2003). PFIRES: A Policy Framework for Information Security. *Communications of the Association for Computing Machinery (ACM)*, pp. 1-18. doi:10.1145/792704.792706

Risk and Vulnerability Analyses for the protection of Information for Future communication security Based Neural. (s.d.).

Saffady, W. (2021). *Managing Information Risks: Threats, Vulnerabilities, and Responses.* United Kingdom: Rowman & Littlefield Publishers.

Safianu, O., Twum, F., & Hayfron-Acquah, J. (2016). Information System Security Threats and Vulnerabilities: Evaluating the Human Factor in Data Protection. *International Journal of Computer Applications, 143*(5), pp. 8-14. doi:10.5120/ijca2016910160

Sinnett, W. M. (2008). *Excellence in Information Integrity.* United States of America: Financial Executives Research Foundation.

Sperstad, I. B., Kjølle, G., & Gjerde, O. (2020). A comprehensive framework for vulnerability analysis of extraordinary events in power systems. *Reliability Engineering and System Safety, 196*, p. 106788. doi:10.1016/j.ress.2019.106788

Steinberg, R. M., Martens, F., Everson, M., & Nottingham, L. (2007). *Gerenciamento de Riscos Corporativos – Estrutura Integrada: Sumário Executivo e Estrutura.* USA: Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Straub, D. W., Goodman, S., & Baskerville , R. (2008). *Information Security. Policy, Processes, and Practices.* United States of America: M.E. Sharpe, Inc. doi:10.1016/B978-0-444-51608-4.X5000-7

Susanto, H., & Almunawar, M. (2018). *Information Security Management Systems. A Novel Framework and Software as a Tool for Compliance with Information Security Standards.* (I. Apple Academic Press, Ed.) Canada: Taylor & Francis Group,LLC.

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions. *Applied Sciences, 10*(12), pp. 1-17. doi:10.3390/app10124102

The Institute of Internal Auditors, Inc., ("The IIA"). (2016). *Global Perspectives: A Auditoria Interna como Conselheira Confiável de Cibernética.* Lake Mary, USA: The Institute of Internal Auditors, Inc., ("The IIA").

The Institute of Internal Auditors, Inc., ("The IIA"). (2019). *Global Perspectives and Insights. 5G e a Quarta Revolução Industrial (Parte 1).* Lake Mary, USA: The Institute of Internal Auditors, Inc., ("The IIA").

Trites, G. (2013). *Information Integrity.* United States: American Institute of Certified Public Accountants (AICPA).

Vilelas, J. (2017). *Investigação. O processo de Construção do Conhecimento* (2ª ed.). Lisboa: Edições Sílabo.

Ward, J. L., & Peppard, J. (2002). *Strategic Planning for Information Systems* (3rd ed.). United Kingdom: John Wiley & Sons Ltd.

Watkins, S. G. (2008). *An Introduction to Information Security and ISO27001. A Pocket Guide.* United Kingdom: IT Governance Publishing.

Whitman, M. E., & Mattord, H. (2017). *Principles of Information Security* (6th ed.). United States of America: Cengage Learning.

Glossário

Acesso: a capacidade de um sujeito ou dispositivo usar, manipular, modificar ou afectar os dados ou a informação. Os utilizadores autorizados têm acesso legal a um sistema, enquanto os hackers têm acesso ilegal. Os controles de acesso regulam essa capacidade.

Activo: O recurso organizacional que está a ser protegido. Um activo pode ser lógico, como um site, informações ou dados; ou um activo pode ser físico, como uma pessoa, sistema de computador ou outro objecto tangível. Activos, e particularmente activos de informação, são o foco dos esforços de segurança.

Agente de ameaça: a instância específica ou um componente de uma ameaça. Por exemplo, todos os hackers do mundo representam uma ameaça colectiva, enquanto um hacker identificado e condenado é um agente de ameaça específico.

Ameaça: Uma categoria de dispositivos, pessoas, software, aplicações ou entidades que representam um perigo para um activo. As ameaças estão sempre presentes e podem ser propositadas ou não direccionadas.

Antivírus - Software utilizado para protecção dos computadores contra *malwares*.

Ataque: Um acto intencional ou não intencional, que pode causar danos ou comprometer as informações e/ ou os sistemas que as suportam. Os ataques podem ser activos ou passivos, intencionais ou não intencionais, directos ou indirectos. Alguém que lê, casualmente, informações sensíveis não destinadas ao seu uso é um ataque passivo. Um hacker a tentar invadir um sistema de informação é um ataque intencional. Um ataque directo é um hacker que utiliza um computador para invadir um sistema. Um ataque indirecto é um hacker a comprometer um sistema e usá-lo para atacar outros sistemas. Os ataques directos originam-se da própria ameaça. Ataques indirectos originam-se de um sistema comprometido ou recurso que não está a funcionar correctamente ou está a funcionar sob o controle de uma ameaça.

Backup: é uma cópia de segurança dos dados, e o seu principal objectivo é manter os arquivos armazenados de forma segura, além de garantir que não haja uma possível perda.

***Cloud*:** refere-se à computação em nuvem, ou seja, à utilização da memória e da capacidade de armazenamento e cálculo de computadores e servidores compartilhados e interligados por meio da internet.

Controle, protecção ou contramedida: mecanismos, políticas ou procedimentos de segurança

que podem conter ataques com sucesso, reduzir riscos, resolver vulnerabilidades e melhorar a segurança dentro de uma organização.

Exploração: Uma técnica usada para comprometer um sistema. Este termo pode ser um verbo ou substantivo. Os agentes de ameaça podem tentar explorar um sistema ou outro activo de informação, usando-o ilegalmente para seu ganho pessoal. Uma exploração pode ser um processo documentado para obter vantagem de uma vulnerabilidade. As explorações fazem uso de ferramentas de software existentes ou componentes de software personalizados.

Exposição: uma condição ou estado de exposição. Em segurança da informação, a exposição existe quando uma vulnerabilidade é conhecida por um invasor e está presente no sistema.

Firewall: é um software de segurança que realiza a verificação de pacotes de dados que são enviados bem como recebidos pelo computador. Assim, ele funciona como um *gatekeeper* digital, verificando os dados que entram e saem.

Firmware: é um conjunto de instruções operacionais que são programadas directamente no hardware de equipamentos electrónicos.

Malware: é um código malicioso e/ ou um programa malicioso de computador destinado a infiltrar-se num sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações.

PAAS: é uma das principais formas de contratar a computação e nuvem, oferecendo as licenças de software, infraestrutura, manutenção, sistema de comunicação e tudo que for necessário para a aplicação, disponibilizando flexibilidade e redução de custos.

Perda: Uma única instância de um activo de informação sofrendo dano ou não intencional ou modificação ou divulgação não autorizada. Quando as informações de uma organização são roubadas, a organização sofreu uma perda.

Perfil de protecção ou postura de segurança: todo o conjunto de controles e salvaguardas, incluindo políticas, formação, conscientização e tecnologia, que a organização implementa (ou não implementa) para proteger o activo.

Risco: a probabilidade de que algo indesejado aconteça. As organizações devem minimizar o risco em conformidade com o grau - quantidade e natureza do risco que a organização está disposta a aceitar.

SAAS: Software como serviço, é uma forma de distribuição e comercialização de software onde o fornecedor será o responsável total da estrutura necessária para utilização e o cliente irá aceder aos serviços pela internet.

Vulnerabilidade: Uma fraqueza ou falha num sistema ou mecanismo de protecção, que se consubstancia numa oportunidade para ser atacado ou danificado. Alguns exemplos de vulnerabilidades são uma falha num pacote de software, uma porta de sistema desprotegida e uma porta destrancada.

Fonte: Adaptado de Whitman & Mattord (2012); Cabral, Bianchi, & Gyenge (2018)

Apêndices

Questionário sobre segurança e integridade da informação em contexto organizacional

O presente questionário foi elaborado no contexto de um trabalho de investigação no Mestrado em Informática e tem como objectivo identificar soluções e comportamentos no âmbito da Segurança e Integridade da Informação em ambiente organizacional. Todos os dados recolhidos serão objecto de tratamento estatístico agregado, e destinam-se exclusivamente a uso académico. São confidenciais e anónimos. A duração do preenchimento do questionário é de aproximadamente 15 minutos. Desde já agradecemos a sua colaboração.

*Obrigatório

1. Género *

Marcar apenas uma oval.

- ◯ Masculino
- ◯ Feminino
- ◯ Não responde

2. Faixa Etária *

Marcar apenas uma oval.

- ◯ 18 - 30
- ◯ 31 - 40
- ◯ 41- 50
- ◯ 51 - 60
- ◯ mais de 60

3. Habilitações *

Marcar apenas uma oval.

- ◯ Ensino básico
- ◯ Ensino secundário
- ◯ Ensino profissional
- ◯ Licenciatura
- ◯ Mestrado ou Doutoramento

4. Actividade Principal da Empresa *

Marcar apenas uma oval.

- ◯ Agricultura, produção animal, caça, silvicultura e pesca
- ◯ Indústrias extractivas
- ◯ Indústrias transformadoras
- ◯ Electricidade, gás e água
- ◯ Construção
- ◯ Comércio por grosso e a retalho
- ◯ Transporte e armazenagem
- ◯ Alojamento, restauração e similares
- ◯ Actividades financeiras e de seguros
- ◯ Actividades imobiliárias
- ◯ Educação
- ◯ Actividades de saúde humana e apoio social
- ◯ Outros sectores

5. Função/Cargo *

_____

6. Antiguidade na Empresa *

Marcar apenas uma oval.

- ◯ menos de 1 ano
- ◯ entre 1 - 5 anos
- ◯ entre 6 - 9 anos
- ◯ entre 10 -20 anos
- ◯ entre 21 - 30 anos
- ◯ mais de 30 anos

No âmbito da política de segurança da informação e dos dispositivos, a sua empresa/entidade:

7. Impõe um sistema de filtragem de mensagens de correio electrónico. *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

8. Impede o acesso dos colaboradores às redes sociais, jogos ou filmes. *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

9. Impede os colaboradores de realizar downloads. *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

10. Impede os colaboradores de alterar a configuração dos equipamentos informáticos. *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

11. Estabelece critérios rigorosos sobre a confidencialidade da informação. *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

Para proteger a segurança da informação e dos dispositivos, a sua empresa/entidade:

12. Impõe a utilização de Antivírus *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

13. Impõe a utilização Antispyware *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

14. Impõe a utilização de Firewall *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

15. Impõe a utilização de VPN (Virtual Private Network) *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

16. Impõe a utilização de Encriptação de mensagens *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

Para proteger a informação recolhida e a sua integridade, a sua empresa/entidade:

17. Impõe critérios para avaliação da credibilidade das fontes *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

18. Impõe critérios sobre a classificação da informação *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

19. Impõe critérios sobre o tratamento da informação *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

20. Impõe critérios sobre o armazenamento da informação *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

21. Impõe critérios para a definição dos acessos *

Conjunto ordenado de elementos (software, hardware, Homem e rede) interligados entre si com o objectivo de permitir acesso a uma zona restrita de um sistema, de utilizadores previamente autorizados

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

Para proteger a informação armazenada e a sua integridade, a sua empresa/entidade:

22. Aceita que seja guardada em disco interno em PC da empresa *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

23. Aceita que seja guardada em disco externo disponibilizado pela empresa *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

24. Aceita que seja guardada em Pen's disponibilizadas pela empresa *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

25. Aceita que seja guardada em serviços de Cloud contratados pela empresa *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

26. Aceita que seja guardada em servidor próprio da empresa *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

Backups

27. Qual das seguintes afirmações caracterizam melhor a periodicidade recomendada pela empresa para a realização de backups. *

Marcar apenas uma oval.

- ◯ Nunca ou raramente
- ◯ Todos os dias
- ◯ Uma a duas vezes por semana
- ◯ Todas as semanas
- ◯ Todos os meses

Para monitorizar a utilização do sistema e as ameaças sofridas, a sua empresa/entidade:

28. Utiliza sistema de IPS (Intrusion Prevention System) *

IPS - recurso que examina o tráfego na rede, para detectar e prevenir os acessos não autorizados na mesma, protegendo-a da exploração das vulnerabilidades.

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

29. Utiliza sistema de IDS (Intrusion Detection System) *

IDS - Recurso que examina o tráfego na rede, para detectar e prevenir os acessos não autorizados na mesma, alertando para comportamentos duvidosos ou ações inesperadas pelos elementos da rede

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

30. Verifica diariamente os incidentes de segurança *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

31. Divulga os incidentes numa base de prevenção e sensibilização dos colaboradores *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

32. Monitoriza todas as acções dos utilizadores dos sistemas internos e externos com acesso por login *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

33. Nos últimos seis meses sofreu algum ataque informático ou acesso indevido resultando na perda de informação ou de horas de trabalho? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

34. Em caso de uma violação do seu acesso, um vírus ou um ataque informático sabe o procedimento a seguir? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

35. Conhece a estrutura de elementos responsáveis pela segurança da informação da empresa? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

36. Como classifica a política de segurança da informação em vigor na empresa? *

Marcar apenas uma oval.

- ◯ Muito Inadequada
- ◯ Inadequada
- ◯ Adequada
- ◯ Muito Adequada

37. Com que frequência são realizadas formações sobre segurança da informação? *

Marcar apenas uma oval.

- ◯ Mensalmente;
- ◯ Trimestralmente
- ◯ Semestralmente
- ◯ Anualmente
- ◯ Nunca ou raramente

38. Com que frequência são feitas acções de formação baseados em incidentes acontecidos? *

Marcar apenas uma oval.

- ◯ Mensalmente
- ◯ Trimestralmente
- ◯ Semestralmente
- ◯ Anualmente
- ◯ Nunca ou raramente

39. Considera que tem necessidade de formação na área da segurança da informação? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

40. Como classifica o seu comportamento no âmbito da segurança e protecção da informação da empresa? *

Marcar apenas uma oval.

	1	2	3	4	5	
Nada prudente	◯	◯	◯	◯	◯	Muito prudente