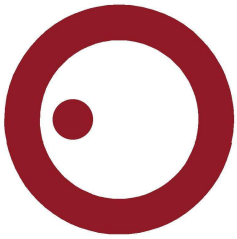


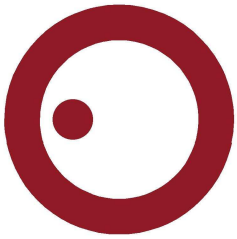
escola superior de tecnologia e gestão
instituto politécnico de leiria

Instituto Politécnico de Leiria
Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança e Informática Forense

MANUAL PRÁTICO PARA PME - CIBERSEGURANÇA, SEGURANÇA DA INFORMAÇÃO, PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

MIGUEL ÂNGELO SARAGOÇA SOARES

Leiria, Setembro de 2023



escola superior de tecnologia e gestão
instituto politécnico de leiria

Instituto Politécnico de Leiria
Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança e Informática Forense

MANUAL PRÁTICO PARA PME - CIBERSEGURANÇA, SEGURANÇA DA INFORMAÇÃO, PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

MIGUEL ÂNGELO SARAGOÇA SOARES
Número: 2210259

Dissertação realizada sob orientação do Professor Doutor Mário Antunes (mario.antunes@ipleiria.pt), da Professora Doutora Marisa Maximiano (marisa.maximiano@ipleiria.pt) e do Professor Ricardo Gomes (ricardo.p.gomes@ipleiria.pt).

Leiria, Setembro de 2023

AGRADECIMENTOS

A edificação da dissertação, mais do que uma pesquisa científica, tratou-se de um trilhar em novos conhecimentos e consolidação de outros, que auxiliará, por certo, o meu contínuo desenvolvimento e aperfeiçoamento profissional. A sua produção, teria sido penosa, sem a valência de um conjunto alargado de pessoas.

Ao Professor Doutor Mário Antunes (mario.antunes@ipleiria.pt), à Professora Doutora Marisa Maximiano (marisa.maximiano@ipleiria.pt) e ao Professor Ricardo Gomes (ricardo.p.gomes@ipleiria.pt) pela orientação, ensinamentos, exigência e apoio científico em momentos-chave, facilitando e tornando viável a consubstanciação da dissertação.

A todos os professores do Mestrado em Cibersegurança e Informática Forense (MCIF), pelos conhecimentos transmitidos, permitindo o aprimorar do meu saber nos domínios lecionados.

Aos meus pais, António e Emília, que providenciaram as ferramentas e a oportunidade de estudar, estando sempre presentes ao longo da vida.

Aos meus filhos, Rafael e Rodrigo, verdadeiras fontes de inspiração e motivação permanente, além do precioso amparo nas questiúnculas relacionados com o LaTeX.

À Susana, companheira de vida, através do inegável e incansável suporte a todas as demandas, nas quais estou envolvido.

Aos colegas do Curso de Mestrado, pelo companheirismo e disponibilidade demonstrada ao longo dos dois anos.

A todos aqueles, que de alguma forma, contribuíram para a elaboração da dissertação, os meus sinceros e proeminentes agradecimentos.

RESUMO

Os ciberataques sofridos pelas empresas portuguesas decorrem em crescendo e os impactos são visíveis e nefastos. Os desafios da cibersegurança são imensos e o espaço público encontra-se inundado com inúmeras soluções tecnológicas, documentação técnica e manuais de boas práticas de múltiplos fabricantes e organismos, que estão, no entanto, tendencialmente descontextualizados da realidade das Micro, Pequena e Média Empresa (PME).

Esta dissertação visa criar um manual prático e direto, constituído por ações e entregáveis, que norteia as PME e permite-lhes edificar um Sistema de Gestão de Segurança e Privacidade da Informação (SGSPI), robusto e resiliente ao cibercrime, e consequentemente, capacitar a organização no cumprimento dos seus objetivos de negócio. Esta dissertação pretende ainda contribuir para a construção de uma verdadeira estratégia e programa de governança de Tecnologia da Informação (TI) direcionada para as PME. É apresentada a metodologia de mapeamento e conceção do portfólio de controlos relacionados com a cibersegurança, segurança da informação, privacidade e proteção de dados pessoais, servindo de motor à perquirição de inúmeras orientações e melhores práticas, normas e regulamentos que perfazem o referencial. O resultado expressa-se num conjunto alargado de artefactos, prontos a serem adotados diretamente pelas PME e que lhes asseverará os mecanismos de controlo e equilíbrios necessários, a mitigar as falhas e brechas de segurança e privacidade da informação.

As normas mais comummente adotadas (e.g., *International Organization for Standardization/International Electrotechnical Commission* (ISO/IEC) 27001, ISO/IEC 27002), são em larga medida generalistas e pouco assertivas face à realidade das PME. Esta dissertação pretende colmatar tal lacuna através do recurso a documentação (e.g., Controlos Críticos do *Computer Emergency Response Team* (CERT) Nova Zelândia (NZ)), que permite construir controlos de maior pragmatismo e com impacto evidente para esta tipologia de empresas.

Palavras-chave: PME, SGSPI, Conformidade, Cibersegurança, Segurança da Informação, Privacidade, Proteção de Dados Pessoais

ABSTRACT

Cyber-attacks suffered by Portuguese companies are happening more often, and the impacts are visible and harmful. The challenges of cybersecurity are immense, and the public space is crowded with numerous technological solutions, technical documentation and good practice manuals of multiple manufacturers and organizations, which are, however, tendentially to be decontextualized from the reality of *Small and Medium-sized Enterprises* (SME).

This dissertation aims to create a practical and direct manual, consisting of actions and deliverables, that guides SME and enables them to build a robust and cybercrime resilient *Information Security and Privacy Management System* (ISPMS), and consequently empower the organization in meeting its business objectives. This dissertation also aims in contributing to build a true *Information Technology* (IT) governance strategy and program targeting the SME. The methodology for mapping and designing the controls portfolio related to cybersecurity, information security, Privacy and Personal Data Protection is presented, serving as a driver for the survey of the numerous frameworks, standards, and regulations that make up the referential. The result is expressed in a wide set of artifacts, ready to be directly adopted by the SME, that will provide them with the necessary control mechanisms and balances to mitigate the security and privacy information failures and breaches.

The most commonly adopted standards (e.g., *International Organization for Standardization/International Electrotechnical Commission* (ISO/IEC) 27001, ISO/IEC 27002), are largely general and not very assertive in relation to the reality of SME. This dissertation aims to fill this gap by using documentation (e.g., Critical Controls of *Computer Emergency Response Team* (CERT) *New Zealand* (NZ)), which makes it possible to build more pragmatic controls with a clear impact on these types of companies.

Keywords: SME, ISPMS, Compliance, Cybersecurity, Information Security, Privacy, Personal Data Protection

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

A	*Availability.*
AEC	Antes da Era Comum.
AES	*Advanced Encryption Standard.*
AIN	Análise de Impacto no Negócio.
AIPD	Avaliação de Impacto sobre a Proteção de Dados.
ANSSI	*Agence Nacionale de la Sécurité des Systèmes d'Information.*
AWS	*Amazon Web Services.*
BCP	*Business Continuity Plan.*
BIA	*Business Impact Analysis.*
BIT	*Binary Digit.*
BSI	*Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security).*
BYOD	*Bring Your Own Device.*
C	*Confidentiality.*
CASB	*Cloud Access Security Broker.*
CC	*Critical Controls.*
CD	*Compact Disc.*
CE	*Cyber Essentials.*
CEN	*European Committee for Standardization.*
CEO	*Chief Executive Officer.*
CERT	*Computer Emergency Response Team.*
CI	*Confidentiality, Integrity.*
CIA	*Confidentiality, Integrity, Availability.*
CIO	*Chief Information Officer.*

CIPT *Certified Information Privacy Technologist.*

CIRC *Computer Incident Response Capability or Center.*

CIRT *Computer Incident Response Team.*

CIS *Center for Internet Security.*

CISA *Cybersecurity and Infrastructure Security Agency.*

CISM *Certified Information Security Manager.*

CISO *Chief Information Security Officer.*

CMM *Capability Maturity Model.*

CNCS Centro Nacional de Cibersegurança.

CNPD Comissão Nacional de Proteção de Dados.

COO *Chief Operating Officer.*

CPU *Central Processing Unit.*

CSA *Cloud Security Alliance.*

CSIRC *Computer Security Incident Response Capability or Center.*

CSIRT *Computer Security Incident Response Team.*

CSO *Chief Security Officer.*

CV *curriculum vitae.*

CVSS *Common Vulnerability Scoring System.*

DHS *Department of Homeland Security.*

DIN *Deutsches Institut für Normung.*

DISA *Defense Information Systems Agency.*

DLP *Data Loss Prevention.*

DOCM *Word Macro-Enabled Document.*

DOD *Department of Defense.*

DPA *Data Processing Agreement.*

DPI *Deep Packet Inspection.*

DPIA *Data Protection Impact Assessment.*

DPO *Data Protection Officer.*

DSS *Data Security Standard.*

DVD	*Digital Video Disc.*
EDR	*Endpoint Detection and Response.*
EOL	End of Life.
EPD	Encarregado de Proteção de Dados.
ERP	*Enterprise Resource Planning.*
EU	*European Union.*
FTP	*File Transfer Protocol.*
GB	Grã-Bretanha.
GDPR	*General Data Protection Regulation.*
GELF	*Graylog Extended Log Format.*
GNUPG	*GNU Privacy Guard.*
GPG4WIN	*GNU Privacy Guard for Windows.*
GPO	*Group Policy Object.*
HTTP	*Hypertext Transfer Protocol.*
I	*Integrity.*
IAC	*Infrastructure as Code.*
IAPP	*International Association of Privacy Professionals.*
ICPA	Identificação, Classificação e Proteção do Ativo.
ICT	*Information and Communication Technology.*
IDPS	*Intrusion Detection / Prevention System.*
IHT	*Incident Handling Team.*
INEM	Instituto Nacional de Emergência Médica.
IOC	*Indicator of Compromise.*
IP	*Internet Protocol.*
IPLEIRIA	Instituto Politécnico de Leiria.

IPS	*Intrusion Prevention System.*
IRC	*Incident Response Center or Incident Response Capability.*
IRT	*Incident Response Team.*
ISACA	*Information Systems Audit and Control Association.*
ISCO	*International Standard Classification of Occupations.*
ISM	*Information Security Manager.*
ISO	*Information Security Officer.*
ISO/IEC	*International Organization for Standardization/International Electrotechnical Commission.*
ISPMS	*Information Security and Privacy Management System.*
IT	*Information Technology.*
KPI	*Key Performance Indicator.*
MCIF	Mestrado em Cibersegurança e Informática Forense.
MFA	*Multi-Factor Authentication.*
MMC	Modelo de Maturidade em Capacitação.
MOOC	*Massive Open Online Courses.*
NAC	*Network Access Control.*
NCSC	*National Cyber Security Centre.*
NIST	*National Institute of Standards and Technology.*
NZ	Nova Zelândia.
OSS	*Open-source Software.*
OTP	Organizacionais, Tecnológicos e Psicológicos.
PAM	*Pluggable Authentication Modules.*
PCI	*Payment Card Industry.*
PCN	Plano de Continuidade de Negócio.
PDCA	*Plan–Do–Check–Act.*

PDF	*Portable Document Format*.
PIB	Produto Interno Bruto.
PIN	*Personal Identification Number*.
PJ	Polícia Judiciária.
PME	Micro, Pequena e Média Empresa.
PPTM	*Excel Macro-Enabled Presentation*.
PRI	Processo de Resposta a Incidentes.
RCMCS	Roteiro de Capacidades Mínimas de Cibersegurança.
RDP	Remote Desktop Protocol.
RGPD	Regulamento Geral sobre a Proteção de Dados.
RH	Recursos Humanos.
RPO	*Recovery Point Objective*.
SA	*System Administrator*.
SBIS	*Small Business Information Security*.
SBOM	*Software Bill of Materials*.
SDN	*Software-Defined Networking*.
SD-WAN	*Software-defined Wide Area Network*.
SERT	*Security Emergency Response Team*.
SGSI	Sistema de Gestão de Segurança da Informação.
SGSPI	Sistema de Gestão de Segurança e Privacidade da Informação.
SIEM	*Security Information and Event Management*.
SIRT	*Security Incident Response Team*.
SMB	*Small and Medium-sized Business*.
SME	*Small and Medium-sized Enterprises*.
SMS	*Short Message Service*.
SMTP	*Simple Mail Transfer Protocol*.
SNMP	*Simple Network Management Protocol*.
SO	Sistema Operativo.

SP *Special Publication.*

SSE *Security Service Edge.*

SSID *Service Set Identifier.*

SSO *Single Sign On.*

STIG *Security Technical Implementation Guides.*

SWG *Secure Web Gateway.*

SWOT *(Strengths, Weaknesses, Opportunities, Threats.*

TCP *Transmission Control Protocol.*

TF *The Fundamentals.*

TI Tecnologia da Informação.

TIC Tecnologia da informação e comunicação.

TLS *Transport Layer Security.*

TTP Táticas, Técnicas, e Procedimentos.

UEBA *User and Entity Behavior Analytics.*

UPS *Uninterruptible Power Supply.*

URL *Uniform Resource Locator.*

US *United States.*

USB *Universal Serial Bus.*

UTM *What Is Unified Threat Management.*

VLAN *Virtual Local Area Network.*

VPN *Virtual Private Network.*

WPA *Wifi Protected Access.*

WSUS *Windows Server Update Services.*

XLSM *Excel Macro-Enabled Workbook.*

ZB *Zettabytes.*

ZTNA *Zero Trust Network Access.*

1

INTRODUÇÃO

Aproximadamente há quarenta e quatro mil anos, a arte rupestre tem a sua génese, dando-se início à feitura rudimentar de informação (Brumm et al., 2021). No entanto, foi preciso esperar até por volta do ano duzentos Antes da Era Comum (AEC), para o surgimento de evidências arqueológicas do uso de formas primitivas em papel, empregando em grande medida o cânhamo (Cartwright, 2017). Os primeiros trabalhos impressos, datam do século oitavo no Japão e o primeiro livro, tal como o concebemos, surge no ano 868 na China (Lechêne, 2020). Durante mais de um milénio, os livros continuam como a principal fonte de armazenamento do conhecimento.

Porém, a segunda metade do século XX conduz à Revolução Digital (Rifkin, 2011) e, a partir desse evento, irrompe uma vaga de poder computacional sem precedentes, tecnologias sem fios, *internet*, aprendizagem automática[1], comunicações e dispositivos móveis, *streaming*, redes sociais, novas formas de organização do trabalho e avanços nas tecnologias de visualização, videojogos, transportes, genética, medicina e exploração espacial. O ano de 1996 revela-se particularmente importante, pela razão, de o aprovisionamento dos dados em suporte digital se tornar menos oneroso do que o armazenamento em papel (Morris e Truskowski, 2003). A informação digital está tão presente em todos os detalhes do quotidiano e sociedade, que a elaboração e difusão do conhecimento manifesta-se irrefreável.

Mesmo observando os números numa escala temporal diminuta, os mesmos deslumbram e falam por si. A cada minuto realizam-se aproximadamente 6 milhões de pesquisas no motor da Google, enviam-se 12 milhões de mensagens por correio eletrónico, 6 milhões de pessoas efetuam compras em plataformas de comércio digital, 452 mil horas de transmissão contínua acontecem através da plataforma Netflix, 240 mil fotos partilham-se no Facebook, e 167 milhões de vídeos são visualizados no TikTok (DOMO, 2022). O número de indivíduos com acesso à *internet* supera a fasquia dos cinco mil milhões e a quantidade total de dados criados, capturados, copiados e consumidos globalmente em 2021, revela-se na grandeza dos 69 *Zettabytes* (ZB). Espera-se que por volta de 2025, a humanidade gerará informação equivalente a 180 ZB. Estes valores são de difícil, mesmo impossível, compreensão para a mente

1 *Machine learning* na designação anglo-saxónica.

humana. Um *zettabyte* representa 8,000,000,000,000,000,000,000 de *bits*. Para melhor idealizar esta cadeia numerológica, conceba-se que cada *bit* é uma moeda de um euro com cerca de três milímetros de espessura. Um ZB composto por uma pilha de moedas, ocuparia a extensão de 2550 anos-luz, o que permitira ir ao sistema estelar mais próximo, Rigil Kentaurus, aproximadamente seiscentas vezes (Cavins, 2022).

Tendo em apreço o mesmo hiato temporal, a McKinsey (2022) prevê que os fluxos de trabalho inteligentes e as interações transparentes entre humanos e máquinas serão provavelmente tão triviais como o balanço da empresa, e a maioria dos colaboradores utilizará os dados para otimizar quase todos os aspetos do seu trabalho. Segundo a Deloitte (2022), os dados têm um valor estratégico incalculável, são um bem crítico e o seu potencial é enorme.

Por outro lado, *"o aumento crescente e exponencial da internet, quer na sua abrangência geográfica, quer no número de utilizadores e na multiplicidade de serviços disponibilizados, encetou vários desafios e potenciou o aparecimento de um vasto leque de ameaças no ciberespaço"* (Mario Antunes e Rodrigues, 2018). Ao estar construída sem uma forma de saber a quem e com o que se está a ligar, expõe o difícil problema da ausência de uma camada de identidade nativa (Cameron, 2005). Deficiência essa, que está na origem de numerosas ameaças à segurança da informação e multiplica o cibercrime pela exploração de vetores de ataques, como o *phishing*, que tem expandido ao longo do tempo (APWG, 2022). Em súmula, a profusão de equipamentos interligados e a sua heterogeneidade, e a imensurabilidade e valor dos dados, potencia a proliferação de cibercriminosos (Espinosa, 2021) e coloca as organizações sob pressão e no radar das partes interessadas (e.g., acionistas, clientes, colaboradores, reguladores).

1.1 MOTIVAÇÃO, PERTINÊNCIA DO TEMA E IDENTIFICAÇÃO DO PROBLEMA

Os recentes e contínuos ciberataques perpetuados a diversos setores do tecido empresarial português (CNCS, 2022) evidenciam, realçam e colocam a descoberto, as fragilidades dos programas de segurança da informação em vigor nas organizações públicas e privadas. A exfiltração de dados pessoais (DN, 2022) e a disrupção do negócio (SAPO, 2022), tendencialmente acarreta prejuízos avultados a nível reputacional e financeiro, podendo mesmo colocar em causa a viabilidade da empresa e em última instância a própria segurança nacional (Lusa/DN, 2022). Em Portugal, conforme os últimos valores disponibilizados pela (Pordata, s.d.), as Micro, Pequena

e Média Empresa (PME)[2], representam 99,9%[3] do tecido empresarial português, são cerca de 1.3 milhões de empresas[4], e o seu volume de negócios ascende aproximadamente a 230 milhões de euros[5]. Escrutinando os dados, pode-se aferir que as PME dominam o mercado e não possuem músculo financeiro suficiente para investimentos avultados, pelo facto, de, em média cada empresa faturar um valor a rondar os 170 mil euros anualmente.

A falta de capacidade das organizações portuguesas em conseguir desenvolver programas de segurança da informação e privacidade dos dados é notória. Em dezembro de 2020, somente noventa empresas apresentavam o selo da distinta certificação *International Organization for Standardization/International Electrotechnical Commission* (ISO/IEC) 27001 (JTC1/SC27, 2022a) em Portugal, consoante a 16.ª edição do GEC – Guia de Empresas Certificadas 2021 – 2022, contendo oitenta páginas de informação, sobre a evolução da certificação no mundo, na Europa e em Portugal (Cempalavras, 2022). É incomodativo indagar, no estudo supracitado, que a Hungria, tendo sensivelmente o mesmo número de habitantes de Portugal e um Produto Interno Bruto (PIB) significativamente inferior, detinha, no mesmo período, quinhentas e sessenta organizações certificadas. Existe, portanto, uma verdadeira desunião entre os objetivos de negócio das organizações e o pilar estratégico da cibersegurança. Afigura-se imperioso sensibilizar e consciencializar o tecido empresarial português, para o mérito da adoção de práticas de segurança e privacidade da informação, como alicerces catalisadores ao cumprimento e sucesso dos planos de negócio.

A relevância da proposta deste trabalho, é a não existência de bibliografia prática no mercado, abordando a implementação de um Sistema de Gestão de Segurança e Privacidade da Informação (SGSPI), que disponibilize o mapeamento dos requisitos normativos em entregáveis. Há inúmeras consultoras que o fazem, através da prestação de serviços em consultadoria. Também existe um vasto leque de livros publicados nacionais e internacionais, que abordam as diferentes normas de suporte aos sistemas de gestão de governação de TI em perspetiva de explanação de conceitos e construção de metodologias e modelos relacionados com as temáticas da

2 Nota do autor: a categoria das micro, pequenas e médias empresas é constituída por organizações que empregam menos de duzentos e cinquenta colaboradores e cujo volume de negócios anual não excede cinquenta milhões de euros ou cujo balanço total anual não ultrapasse quarenta e três milhões de euros (Commission et al., 2020).

3 https://www.pordata.pt/portugal/pequenas+e+medias+empresas+em+percentagem+do+total+de+empresas+total+e+por+dimensao-2859

4 https://www.pordata.pt/portugal/pequenas+e+medias+empresas+total+e+por+dimensao-2927

5 https://www.pordata.pt/portugal/volume+de+negocios+das+pequenas+e+medias+empresas+total+e+por+dimensao-2932

cibersegurança, segurança da informação, privacidade e proteção de dados pessoais. No entanto, tanto as consultoras, como os autores, sempre ignoraram, fundamentalmente por motivos pecuniários, os entregáveis, i.e., os *templates* que permitem materializar os aspetos teóricos por eles propostos. O teor da dissertação, centra-se na problemática da construção de um SGSPI compatível com a realidade das PME nacionais, munindo-as dos conhecimentos e entregáveis fundamentais ao sucesso de tal empreitada, ou seja, capacitando-as na implementação de soluções robustas e práticas em torno das áreas da cibersegurança e proteção de dados.

1.2 RESULTADOS ESPERADOS

Esta proposta, aspira criar um manual acessível, prático e objetivo, de como as PME portuguesas, podem implementar autonomamente um SGSPI. É expectável que um só colaborador ou uma pequena equipa, consiga, com parcos recursos, conceber um sistema de cibersegurança funcional visando o negócio e em consonância com as melhores práticas normativas existentes. Ao longo das inúmeras etapas do processo, é disponibilizada toda a documentação necessária, que dá suporte prático à ação ou ações solicitadas. Ao se formular o porquê da racionalidade subjacente à criação da Política de Segurança e Privacidade da Informação, é fornecido um guião para essa política. Por exemplo, anunciando-se o requisito de existir um registo dos incidentes de segurança e privacidade da informação, é entregue o documento para esse efeito, contemplado todos os campos e atributos correspondentes, incluindo a forma do seu preenchimento. E assim sucessivamente, para cada atividade do processo de construção do ecossistema de segurança e privacidade da informação, serão disponibilizados os entregáveis necessários (e.g., registos, formulários, modelos, listas de verificação, políticas), devidamente preenchidos, com a adequada justificação (i.e., o porquê da necessidade) e referências apropriadas (i.e., qual a norma, padrão ou enquadramento de suporte).

Mais do que um roteiro, uma norma ou um manuscrito sobre cibersegurança, pretende-se disponibilizar um manual de referência, que seja adotado pelas PME nacionais e que lhes permita alavancar e fabricar um programa de ciber-resiliência, não apenas descrevendo o que fazer, mas como o devem empreender, e disponibilizando-lhes as ferramentas requeridas.

Outro resultado expectável derivado do anteriormente mencionado, é o das organizações aumentarem o nível de robustez intrínseca às ameaças do mundo tangível e digital, através da aplicação das propostas apresentadas pelo autor nesta

dissertação. Desta forma poderão anular ou minimizar os riscos humanos, processuais e tecnológicos, que possam colocar em causa a estratégia delineada para o negócio.

Pretende-se ainda com esta dissertação proporcionar aos auditores e gestores de conformidade, a avaliação da completude dos sistemas de gestão onde têm intervenção, face ao explanado nas secções subsequentes. Aspira-se desta forma contribuir para a democratização da implementação dos sistemas de gestão, em particular, dos de segurança e privacidade.

Inúmeras vezes, a comunidade de especialistas em cibersegurança, incorpora entropia desnecessária ao processo de aquisição e transmissão do conhecimento. Tal acontece quer por interesses comerciais, quer por tentar manter o conhecimento restrito aos seus pares, quer ainda por falta de capacidade ou arte em simplificar. A premissa subjacente ao desenvolvimento desta dissertação, é facilitar e desconstruir conceitos complexos em ações práticas compreensíveis às partes interessadas menos familiarizadas com os tópicos da cibersegurança, segurança da informação, privacidade e proteção de dados pessoais. Não menos importante, é colocar o foco na realidade portuguesa, ou seja, na dimensão socioeconómica das empresas e na legislação nacional e expectativas dos reguladores (e.g., Comissão Nacional de Proteção de Dados (CNPD), Centro Nacional de Cibersegurança (CNCS)).

Sob outra perspetiva, embora de menor relevância por o enfoque estar no exercício e não no processo, pretende-se possibilitar às empresas uma preparação prévia, para obterem uma certificação de terceira parte em segurança e privacidade da informação, como no caso da ISO/IEC 27701 (JTC1/SC27, 2019) e por inerência, no Regulamento Geral sobre a Proteção de Dados (RGPD) (EUR-Lex, 2016).

1.3 MOTIVAÇÕES PESSOAIS

O autor do trabalho possui experiência profissional superior a uma década na implementação, gestão e auditoria de sistemas ISO/IEC 27001 e mais recentemente de RGPD, tendo mesmo, conceptualizado um programa de implementação do Regulamento em várias organizações privadas e institutos públicos. Também concluiu, com sucesso, a primeira implementação da ISO/IEC 27701, numa organização privada em Portugal (em plena pandemia), incluindo a certificação da APCER[6]. Por fim, pretende-se que a produção da dissertação, nomeadamente a metodologia e o conjunto de normas analisadas no presente e futuro, sirvam de firmamento e

6 https://www.apcergroup.com/pt/

processo de sistematização na elaboração de controlos de proteção eficazes, nas atividades exercidas de carácter profissional.

1.4 AUDIÊNCIA

Esta dissertação tem a intenção de servir um grupo diversificado de profissionais[7] na esfera da cibersegurança, nomeadamente:

- Indivíduos com responsabilidades na gestão de risco, objetivos de negócio e estratégia corporativa (e.g., *Chief Executive Officer* (CEO), *Chief Operating Officer* (COO), *Chief Information Officer* (CIO));
- Indivíduos com responsabilidades na conceção, operacionalização, gestão e melhoria contínua do programa de cibersegurança da organização (e.g., *Chief Information Security Officer* (CISO), *Chief Security Officer* (CSO), *Information Security Officer* (ISO));
- Indivíduos com responsabilidades na arquitetura, implementação, avaliação e monitorização de ativos de informação (e.g., arquitetos de soluções informáticas, engenheiros de segurança da informação, auditores);
- Indivíduos com responsabilidades na liderança de equipas, departamentos, unidades de negócio e funções relevantes (e.g., gestores de negócios, diretores, responsáveis de projetos).

1.5 ORGANIZAÇÃO DOS CAPÍTULOS

A dissertação está desenhada para nortear o leitor por um processo lógico de enquadramento da temática. O primeiro capítulo debruça-se na motivação para a escrita da dissertação e na descrição da pertinência no contexto atual e problemática que se pretende solucionar. Ainda no primeiro capítulo são sintetizados os resultados esperados, após a aplicação prática da metodologia anunciada na dissertação, bem como as motivações do autor e a apresentação do público alvo.

Os conteúdos remanescentes da dissertação, estão dispostos no formato subsequente:

7 Nota do autor: a nomenclatura dos cargos não é necessariamente designada de forma igual em cada organização, tendo-se optado por seguir, sempre que possível, a classificação adotada pelo *International Standard Classification of Occupations* (ISCO) disponível em https://isco-ilo.netlify.app/en/isco-08/. Cada empresa deverá espelhar os títulos de trabalho descritos ao seu contexto.

- O capítulo 2 detalha ensaios de inúmeros autores gravitando em redor dos temas da dissertação em apreço. Os textos são agrupados nas temáticas de Cibersegurança, Privacidade e Proteção de Dados Pessoais, e Segurança da Informação. São divulgadas num quadro resumo as valências, bem como, os lapsos de cada um dos trabalhos de natureza técnico-científica analisados.
- O capítulo 3 providencia a materialização do método, detalhando em pormenor as suas múltiplas etapas, desde a bibliografia à construção das regras de seleção dos controlos, passando pela matriz de mapeamento e encerrando no catálogo de ações.
- O capítulo 4 amplifica, desenvolve e expõe a cartografia e o portfólio de controlos, materializando um programa prático de ciber-resiliência com foco nas PME.
- O capítulo 5 corrobora a execução prática do roteiro de controlos numa empresa nacional, especializada na oferta de soluções e serviços de TI na área dos ERP.
- O capítulo 6 escrutina em retrospetiva a dissertação, debruçando-se sobre os resultados alcançados e traçando as linhas orientadoras para um trabalho futuro, tais como, a inclusão de determinados *frameworks*, o refinamento do portfólio criado e a materialização do conceito no tecido empresarial português das PME.
- Por fim os apêndices A a Z suportam e sustentam algumas partes assinaladas na dissertação, através dos inúmeros artefactos recolhidos, identificados e analisados.

2

TRABALHO RELACIONADO

Na bibliografia de suporte à dissertação, encontra-se um vasto conjunto de literatura especializada adicional, às infracitadas, abordando assuntos em redor da temática em perquirição, não sendo objeto de análise no capítulo em curso. São normas, *frameworks* e outros documentos, amplamente divulgados e conceituados aos que se dedicam academicamente e profissionalmente a estes motes. O somatório e fusão de todas as peças bibliográficas, permitem capacitar o autor, com as ferramentas necessárias à elaboração da dissertação.

Tanto quanto é do conhecimento do autor, não foi identificado qualquer trabalho específico sobre a temática em apreciação, no entanto, encontraram-se, na lista de repositórios esquadrinhados com recurso à metodologia desenvolvida no capítulo 3, um número considerável de artigos relacionados, preeminentes na balização e enquadramento da dissertação em apreço.

O conhecimento sondado, alicerça-se e encontra-se agrupado nas temáticas macro em estudo, i.e, Cibersegurança, Privacidade e Proteção de Dados Pessoais, e Segurança da Informação.

2.1 CIBERSEGURANÇA

O artigo de Alharbi et al. em *«The Impact of Cybersecurity Practices on Cyberattack Damage: The Perspective of Small Enterprises in Saudi Arabia»* (Alharbi et al., 2021) determina o impacto de várias práticas de segurança, nos danos causados pelos ciberataques, especialmente nas pequenas empresas da Arábia Saudita. Foram selecionadas três variáveis dependentes para medir os danos causados por ataques de cibersegurança, nomeadamente danos financeiros, perda de dados sensíveis, e tempo de recuperação. Além disso, doze práticas de segurança foram elegidas como variáveis independentes:

1. Sensibilização em cibersegurança;
2. Conhecimento dos danos da cibersegurança;

3. Governança em cibersegurança;
4. Aplicação de políticas em cibersegurança;
5. Uso de sistemas de proteção;
6. Seguir procedimentos de cibersegurança;
7. Treino especializado em cibersegurança;
8. Contacto com autoridades em cibersegurança;
9. Equipa de inspeção[1];
10. Plano de recuperação;
11. Custo do *software* de proteção;
12. Salários dos profissionais.

Os autores propõem uma *framework*, que relacione a interligação entre as variáveis (in)dependentes. Empresas que tenham os vetores (ix) e (x) estão menos propensas a sofrerem danos financeiros. Por outro lado, em relação à perda de dados sensíveis, as variáveis (vii) e (xii) minimizam tais ocorrências. Por fim, o tempo de recuperação tem mais ganhos com as constantes (viii) e (ix).

Este documento contribui com a enumeração das práticas mais eficazes de supressão de riscos cibernéticos, que as pequenas empresas devem adotar. Por outro lado, peca pela falta de desdobramento das práticas em ações mensuráveis.

A dissertação de Chak, *«Managing cybersecurity as a business risk for small and medium enterprises»* (Chak, 2015), analisa três soluções, para que as PME consigam gerir os riscos de cibersegurança, sem terem necessariamente de realizar fortes investimentos em soluções técnicas. O cibercrime já não pode ser considerado uma ameaça, que consiga ser gerida eficazmente numa base individual, especialmente para as PME, pelo investimento de grande envergadura na gestão individual dos riscos. Assim, o autor propõe: (i) Policiamento de comunidade[2] — conceito que enfatiza o trabalho em parceira entre a polícia e as comunidades, para reforçar a sensação de segurança e confiança, de modo a reduzir a criminalidade. Argumenta-se que a adaptação do policiamento comunitário do mundo real, pode ser aplicado no ciberespaço, para aumentar a ordem jurídica e transmitir uma sensação de segurança a todas as empresas, especialmente as PME; (ii) Ciber-seguro — as PME têm escassos recursos financeiros e humanos e um seguro informático, é um dos instrumentos a serem adotados numa estratégia compreensiva de gestão de

1 Nota do autor: entenda-se equipa de operações em segurança, habilitada a inspecionar atividades de cibersegurança.
2 *Community policing* em designação anglo-saxónica.

risco; (iii) Higiene cibernética — melhora a cibersegurança pela incorporação da gestão de comportamento do utilizador final, em vez de uma dependência excessiva sobre tecnologia automatizada. O autor refere, que oitenta a noventa porcento das violações de redes empresariais, requerem somente técnicas básicas de intrusão.

Este documento contribui com três controlos de investimento módico, a serem acolhidos pelas pequenas organizações. Por outro lado, peca pela não materialização dos controlos propostos em afazeres tangíveis.

Carmo Quaresma em «Monitorização de eventos numa PME» (Carmo Quaresma, 2014) contextualiza as funcionalidades, capacidades e vantagens criadas pela utilização de programas de código aberto[3], livre de licenciamento, por parte das PME, já com alguma dimensão. A implementação sem custos de programas associados e documentação completa, para facilitar posteriores alterações, são alguns dos requisitos na seleção de ferramentas, que o autor menciona. A escolha recai sobre o *software* Zabbix[4], que obteve a pontuação mais elevada, dos critérios definidos.

Este documento contribui na democratização das soluções de código aberto, de custo ínfimo, face aos programas ditos comerciais. Por outro lado, peca no reduzido leque de observações efetuadas.

O relatório de Cook sobre *«Effective Cyber Security Strategies for SmallBusinesses»* (Cook, 2017) explora as estratégias de quatro pequenas empresas, que com sucesso, adotam medidas de proteção dos seus negócios face a prováveis ciberataques. Empregam menos de duzentos e cinquenta trabalhadores, faturam até dez milhões de dólares, utilizam a *internet* nas operações de negócio e implementam com sucesso estratégias de cibersegurança. Os resultados apontam no sentido, que uma estratégia de sucesso contra o cibercrime, alicerça-se em três dimensões: (i) Desenvolver e implementar um plano estratégico compreensivo de cibersegurança; (ii) Confiar em parceiros de negócio no fornecimento de soluções de TI especializadas e proteção cibernética; (iii) Sensibilização em cibersegurança. Cada uma destas dimensões subdivide-se num conjunto de tarefas descritas no texto. De outro autor, são ilustrados seis passos de segurança, que os donos de pequenos negócios devem tomar, de modo a se protegerem (Cook, 2017, p. 103).

Este documento contribui com o destrinçar de fatores eficazes face ao cibercrime. Por outro lado, peca na não ilustração dos passos necessários a assegurar essa eficácia.

3 *Open-source Software* (OSS) em designação anglo-saxónica.
4 https://www.zabbix.com/

A tese de mestrado do Jideani em *«Towards a cybersecurity framework for South African e-retail organizations»* (Jideani, 2018) realça a mitigação de ocorrências de ciberataques nas PME de retalho. Quais os desafios específicos da cibersegurança e como se podem mitigar, são questões, que o autor visa desbravar ao longo do ensaio. São enumeradas seis estratégias de mitigação: (i) Processos e procedimentos de proteção da informação; (ii) Estratégia de gestão de risco; (iii) Sensibilização e formação; (iv) Conformidade; (v) Controlo de acessos; (vi) Monitorização contínua de segurança. Igualmente é proposta uma *framework* de cibersegurança para o retalho eletrónico (Jideani, 2018, p. 112).

Este documento contribui com uma nova *framework* e estratégias de contenção relativas a ciberataques. Por outro lado, peca por não apresentar a materialização das estratégias.

A exposição de Matos no texto «Cibersegurança: políticas públicas para uma cultura de cibersegurança nas empresas» (Matos, 2018) debruça-se sobre como podem as empresas portuguesas, em especial as PME, lidar com os riscos de cibersegurança e, face ao quadro de políticas públicas (inter)nacionais, que instrumentos têm ao seu dispor para tal. Destaca-se o relato da evolução do número de participações de crimes informáticos em Portugal, que tem subido, e um quadro com oito etapas para a implementação de uma cultura de cibersegurança nas organizações. No entanto, é apresentado numa magnitude genérica sem materialização de ações.

Este documento contribui com diligências na concretização de uma cultura empresarial de proteção face a ciberataques. Por outro lado, peca por não trilhar o caminho efetivo no processo de disrupção cultural necessário a tal empreitada.

A narrativa de Nabila quanto a *«The Impact of Cyber Security on SMEs»* (Nabila, 2014) apresenta uma metodologia sustentada na procura em bases de dados *online* Scopus[5] e Google Scholar[6] sobre cibersegurança. Primeiro, a procura baseia-se nos termos *SME IT Security*, *Small Medium Enterprises IT security* e *Small Medium Business IT security*. Segundo, consubstânciou-se uma refinação da pesquisa anteriormente obtida, pela utilização dos vocábulos *Security*, *Survey*, *Culture*, *Risk*, *Assessment*, *Policy*, e do operador *AND* com os termos do primeiro passo. Terceiro, pela revisão dos resumos e conclusões das fontes de informação. O estudo afunila em duas dimensões e no seu impacto, ameaças e prevenção para as SME: computação em nuvem[7] e no traga o seu próprio dispositivo[8]. É apresentado um questionário,

5 https://www.scopus.com/home.uri
6 https://scholar.google.com/
7 *Cloud comptuing* na designação anglo-saxónica.
8 *Bring Your Own Device* (BYOD) na designação anglo-saxónica

onde se fica conhecedor das tecnologias que as organizações usam na segurança das TI e quais as políticas de cibersegurança em vigor.

Este documento contribui com um método de procura de informação. Por outro lado, peca por apresentar um âmbito parco, resumido a duas tecnologias.

A averiguação de Offers titulada *«Understanding factors influencing SME's decision makers when implementing cybersecurity measures: a protection motivation perspective»* (Offers, 2020) tem a razão de conhecer o que motiva as PME Holandesas a decidirem implementar medidas de proteção em cibersegurança. Para isso utiliza conceitos derivados da *Protection Motivation Theory*[9]. Há conceitos com impactos significativos positivos ou negativos. Do lado positivo temos as variáveis de perceção da gravidade e de perceção da autoeficácia, enquanto do lado negativo, a perceção da vulnerabilidade e a perceção dos custos de resposta. Por exemplo, a perceção de elevados custos de resposta, em termos de tempo, esforço e custo monetário, na implementação de medidas de cibersegurança, apresenta uma relação negativa com a implementação das tais medidas.

Este documento contribui no discernimento das variáveis que influenciam positiva e negativamente a concretização de medidas evasivas a ataques maliciosos. Por outro lado, peca pela utilidade prática duvidosa para com as PME.

A exposição de Saber relativa a *«Determining Small Business Cybersecurity Strategies to Prevent Data Breaches»* (Saber, 2016) foca-se na questão das estratégias de cibersegurança, que os líderes das pequenas empresas implementam para proteger os seus sistemas de violações de dados. A recolha de informação efetua-se por um questionário *online*, contendo perguntas abertas, aos líderes de cinco PME, seguida de entrevistas cara-a-cara semiestruturadas. Três categorias primordiais identificadas: (i) Política — envolve a importância das PME em terem políticas de cibersegurança em prática; (ii) Formação — contribui para a relevância das PME em consciencializar os colaboradores em relação às ameaças de cibersegurança; (iii) Tecnologia — destaca a importância da dependência em *hardware* e *software* pelas PME. Menciona-se um método de outros autores, para criar, implementar e fazer cumprir um plano de segurança da informação a custo diminuto nos pequenos negócios (Saber, 2016, p. 23). Também é descrita uma lista de verificação na interrogação a executivos, de modo a obter uma medição precisa da eficácia da resiliência cibernética (Saber, 2016, p. 35).

9 https://doi.org/10.1080/00223980.1975.9915803

Este documento contribui com a identificação de quais as medidas adotadas por pequenos negócios, no combate ao cibercrime. Por outro lado, peca pela incapacidade em esmiuçar quais as políticas, formações e tecnologias a adotar.

O escrito de Silva Baptista designado «O fator humano na cibersegurança» (Silva Baptista, 2017) contribui para o despertar da consciencialização em cibersegurança, sendo este o ponto de partida para o desenvolvimento de um programa de capacitação de cidadãos em cibersegurança. Uma organização que investe na formação em cibersegurança dos seus funcionários é uma organização que fomenta o desenvolvimento das competências, fornecendo relevantes conhecimentos e proficiências de segurança da informação. São citadas informações interessantes, como *"60% das PME encerram a sua atividade, seis meses após um efetivo ataque de cibersegurança."* e *"cerca de 80% dos ataques ocorridos, tiveram como fundamento a falta de boas práticas de cibersegurança nas organizações"*. Abordam-se os principais programas de capacitação em cibersegurança, a relação dos *Massive Open Online Courses* (MOOC), do *e-learning* e a cibersegurança. O ponto central da tese é, quiçá, a introdução de uma tabela das dimensões em cibersegurança, que mostra por segmentos da sociedade (função profissional), as necessidades e o nível de competências em cibersegurança a adquirir (A — Alto, M — Médio, B — Baixo), subdividas por vetores de ação.

Este documento contribui com um quadro revelador do grau de sensibilização e consciencialização em cibersegurança, que determinada função profissional requer. Por outro lado, peca por falhar em apresentar um programa com tarefas, métricas e objetivos a serem conseguidos pelas empresas.

A dissertação de Whitehead quanto a *«Investigation of factors influencing cybersecurity decision making in Irish SME's from a senior manager/owner perspective»* (Whitehead, 2020) utiliza a análise qualitativa e fornece uma contribuição para a teoria sobre as perceções de cinco gestores de PME da Irlanda, quando confortados com decisões de investimento em cibersegurança. Conclui-se que seis fatores influenciam as decisões: (i) custo; (ii) reputação da empresa; (iii) perda monetária; (iv) sensibilização; (v) regulamentação; (vi) perícia. Os fatores delineados não são independentes uns dos outros. Cada um tem uma relação no processo de tomada de decisão, mas a ponderação altera-se para diferentes organizações. A principal preocupação dos gestores de topo, prende-se com o fator reputação da empresa. A investigação mostra que as PME reconhecem a necessidade de investir e estão dispostos a tal, mas é necessário maior orientação, assegurando investimento nas áreas mais impactantes para o negócio.

Este documento contribui com os coeficientes fulcrais nas decisões de investimento em cibersegurança. Por outro lado, peca por não descriminar quais os investimentos que minimizam e maximizam os coeficientes.

O exercício de Zec intitulado «Cyber security Measures in SMEs: a study of IT professionals' organizational cyber security awareness» (Zec, 2015) visa providenciar novos conhecimentos no que respeita aos aspetos Organizacionais, Tecnológicos e Psicológicos (OTP) da cibersegurança, nomeadamente sobre como influenciam as PME. O relatório mostra um sumário de *frameworks* teóricas e suas particularidades sobre a cibersegurança e desenvolve uma nova *framework*. Realiza um questionário a algumas PME e agrupa as respostas em cada um dos vetores OTP. A dimensão psicológica, menos trivial, estuda questões como a (in)capacidade de reportar e abordar a falta de sapiência em cibersegurança à gestão de topo e de dar conhecimento sobre a resolução de uma exfiltração dados, apesar de ninguém ter tido consciência de tal ocorrência. Em suma, debruça-se sobre os fatores culpa e vergonha. Mais diretamente relacionado com a dissertação em curso, responde à pergunta de quais as razões das PME estarem mais expostas a ciberataques, do que as grandes empresas: (i) Parco investimento financeiro; (ii) Não cumprimento na sua plenitude do aspeto tecnológico da segurança cibernética; (iii) Insuficiente educação dos profissionais de TI; (iv) Insatisfatória segregação de funções nas TI. Os profissionais estão dedicados à globalidade das Tecnologia da informação e comunicação[10] e não somente às tarefas de cibersegurança; (v) Não sensibilização e consciencialização para os três pilares OTP da cibersegurança e os mesmos são tratados desigualmente; (vi) Negligência no cumprimento de tarefas, não as executando, mesmo sabendo que devem; (vii) Falta de capacitação dos profissionais de TI por parte dos gestores, especialmente no tocante à implementação de normas cibernéticas.

Este documento contribui com uma mescla de indicadores da causa das PME encontrarem-se mais voláteis a ciberataques. Por outro lado, peca pela ausência de pragmatismo.

2.2 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

A investigação de Alvega sobre *«Privacy awareness in Portuguese SMEs»* (Alvega, 2021) assenta na realização de um inquérito para a avaliação do nível de sensibilização das PME Portuguesas face ao RGPD. Neste estudo afere-se que uma percentagem significativa não aplica medidas técnicas e organizacionais, na

10 *Information and Communication Technology* em designação anglo-saxónica.

mitigação de riscos relacionados com a proteção de dados pessoais. Também se evidenciam as dificuldades das PME em configurar robustamente componentes de infraestrutura (e.g., barreiras de segurança[11]), efetuarem as respetivas atualizações, testarem a fiabilidade dos dados salvaguardados e ausência de procedimentos em caso de comprometimento. O estudo ainda apresenta um conjunto de recomendações para as PME sobre parametrizações a serem efetuadas em barreiras de segurança e recomenda algumas aplicações.

Este documento contribui na aferição de dificuldades das PME Portuguesas na consumação do RGPD. Por outro lado, peca pelo afunilamento somente nas soluções de perímetro.

O trabalho de Ashraf em *«GDPR Implementation Framework for SMEs»* (Ashraf, 2021) avalia a disponibilidade de *frameworks* e ferramentas para assegurar a conformidade das PME face ao RGPD, e propõe uma nova *framework* simplificada para empresas até cem colaboradores e com um orçamento inferior a cem mil euros, no intuito de asseverar a concordância perante o Regulamento. O relatório debruça-se em detalhe na ferramenta de avaliação do RGPD da Microsoft[12] e superficialmente nas *Innovative Routines International* GDPR *Compliance ToolKit* (IRI, s.d.) e GDPR.EU *Checklist and Recommendations* (ProtonTechnologies, s.d.). A partir da página 36, formula a resposta de conformidade ao Regulamento através de uma metodologia fabricada por si, intitulada GDPR *Compliance Framework for* SME alicerçada nos seguintes passos: (i) Definição de todas as atividades envolvendo dados pessoais e as razões de legitimidade ao seu tratamento; (ii) Avaliação de Impacto sobre a Proteção de Dados[13]; (iii) Nomeação de um Encarregado de Proteção de Dados[14] quando necessário; (iv) Acordo de tratamento de dados pessoais em subcontratação[15]; (v) Plano de Continuidade de Negócio[16]; (vi) GDPR *Security Incident Process*.

Este documento contribui com uma *framework* simplicada na busca da conformidade perante o RGPD nas PME. Por outro lado, peca por não endereçar todos os requisitos subjacentes ao Regulamento. Por exemplo, os direitos dos titulares dos dados compreendidos entre o artigo 12.º e o 23.º não são tidos em consideração no programa apresentado pelo autor.

11 *Firewall* na designação anglo-saxónica.
12 www.microsoft.com
13 *Data Protection Impact Assessment* na designação anglo-saxónica.
14 *Data Protection Officer* na designação anglo-saxónica.
15 *Data Processing Agreement* na designação anglo-saxónica.
16 *Business Continuity Plan* na designação anglo-saxónica.

A dissertação de Carvalho Silva com o título «RGPD aplicado nas PME portuguesas» (Carvalho Silva, 2020) conduz um inquérito a 772 PME, visando avaliar que tipo de dados estas tratam, o conhecimento que têm do regulamento e como se adaptaram as novas regras. Pelo estudo efetuado, denota-se, que quanto mais pequena é a organização, maior a dificuldade em obter conhecimento das alterações e imposições legislativas. Apresenta-se uma tabela com onze tipos de categorias de dados pessoais, tendo-se solicitado às empresas a indicação dos dados tratados. As informações de identificação, financeiras, rastreamento e sociais surgem no topo. Em relação às finalidades para o tratamento de dados, a gestão de clientes e prestação de serviços aparece em primeiro lugar. Por outro lado, o cumprimento de obrigações legais é o fundamento de licitude mais apontado pelas empresas. É interessante constatar, que cerca de 75% das organizações não efetuaram uma auditoria aos dados pessoais que detêm. Nas medidas tomadas para cumprimento do Regulamento, a ação de alteração de procedimentos internos encabeça a lista anunciada. É possível ainda verificar, que apenas cerca de 20% das PME demonstrarem algum tipo de preocupação em relação às coimas.

Este documento contribui na perceção do nível de implementação do RGPD nas PME. Por outro lado, peca por não exibir uma estratégia de como empreender o Regulamento nos processos das empresas.

O estudo de Fischer designado *«Guidelines for SME adaption to GDPR Case study of Evalent»* (Fischer, 2020) contribui com linhas orientativas e ações práticas na implementação do RGPD em PME. Os motores de pesquisa e base de dados foram varridas na procura de *frameworks* e guias existentes na execução do Regulamento. Palavras-chave usadas: "GDPR", "GDPR *compliance*", "GDPR *implementation*", "GDPR *guidelines*", "GDPR *framework*", "GDPR *compliance guidelines*", "GDPR *compliance framework*", "GDPR *compliance guidelines*", e "GDPR *compliance framework*". Guias estudados: "APSs GDPR *FRAMEWORK*", "*Framework for Demonstrable* GDPR *Compliance A mapping of the Nymity's Privacy Management Accountability Framework to* GDPR *Compliance Obligations*", "IBMs GDPR *framework*", "*Copenhagen Compliance* GDPR *framework*", e "*Information commission framework*". A *framework Nymity's Privacy Management Accountability Framework*[17] é a selecionada pelo autor, por ser a mais completa, a ser usada como caso de estudo na empresa Evalent. É apresentado a partir da página 90, as diretrizes de implementação do Regulamento com base no ciclo *Plan–Do–Check–Act*. A partir

17 Nota do autor: é delicioso constatar, que o autor da presente dissertação, com uma antecedência de quatros anos, optou pelo mesmo esboço, como um dos modelos fulcrais à construção de uma *framework* de implementação do RGPD para as empresas nacionais.

da página 122, ilustra-se alguns entregáveis, nomeadamente: (i) GDPR *policy*; (ii) *Security policy*; (iii) *Hosting policy*; (iv) GDPR *routines and checklists*.

Este documento contribui com ações práticas no cumprimento do RGPD nas PME. Por outro lado, peca por um conjunto parcimonioso de entregáveis.

2.3 SEGURANÇA DA INFORMAÇÃO

A resenha de Mário Antunes et al. cognominada *«Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal»* (Mário Antunes et al., 2021) difunde um projeto de gestão de segurança da informação e cibersegurança, no qual uma metodologia baseada na conhecida norma ISO/IEC 27001:2013 é concebida e implementada em cinquenta PME localizadas na região centro de Portugal. As famílias de controlos do anexo A, são assignadas a dois perfis. O perfil *Standard* engloba os conjuntos de controlos A.5, A.8, A.9, A.10, A.12, A.13, A.14 e A.18. Por seu lado, o perfil Completo incorpora a totalidade dos controlos A.5 a A.18. Constata-se, pela positiva, que a formulação da *framework* e a sua posterior arguição foi entregue ao meio académico, enquanto a componente experimental a consultoras de TI.

De notar, que as empresas submetidas a tal escrutínio, não se tornam totalmente preparadas para serem submetidas a um processo de certificação, não sendo esse um objetivo do projeto. Também é possível depreender que os controlos dependentes de processos e documentação são significativamente mais fáceis de cumprir, em comparação com os que são mais tecnológicos e existe a necessidade intrínseca de se instalar equipamento adicional e de implementar procedimentos técnicos mais refinados. Este facto está relacionado com o normativo ser *"difícil de aplicar a PME"*.

As microempresas apresentam o rácio menos elevado de controlos avaliados positivamente, enquanto as empresas exportadoras obtêm o melhor desempenho. O que não é de estranhar, pelas obrigações de conformidade ao longo da cadeia de fornecimento. Os autores relatam a importância de se observarem outras melhores práticas e *frameworks* de modo a se validar se o normativo em estudo, é o mais adequado. Um ponto igualmente relevante, é a importância a se dar à formação e certificação dos colaboradores das PME.

Este documento contribui para assimilar as dificuldades das PME em construirem um SGSI baseado em exclusivo na norma ISO/IEC 27001. Por outro lado, peca pelo descartar dos requisitos das secções quatro a dez e o não foco nos entregáveis.

O escrito realizado por Azinheira sobre «Desenvolvimento de uma metodologia para avaliação do estado da segurança informática em PME» (Azinheira, 2022) descreve uma metodologia para o mapeamento do Roteiro de Capacidades Mínimas de Cibersegurança (RCMCS) facultado pelo Centro Nacional de Cibersegurança (CNCS), com as sugestões da norma internacional ISO 27001:2013. O principal objetivo passa por identificar os pontos de convergência e correlações entre as ações do roteiro e da norma. Os graus de correlação, dividem-se em três: (i) Ação — (AC): tanto o roteiro como a norma sugerem as mesmas ações ou muito semelhantes; (ii) Alvo — (AL): tanto o roteiro como a norma têm o mesmo objetivo final, mesmo que as ações sugeridas difiram; (iii) Âmbito — (AM): tanto o roteiro como a norma têm o mesmo âmbito, mas as ações ou mesmo o objetivo final explícito são diferentes.

Embora o autor mencione a ISO/IEC 27001, o conteúdo é objetivamente da ISO/IEC 27002. A ISO/IEC 27001 tem o foco nas fundações de um Sistema de Gestão de Segurança da Informação (SGSI) constituído por requisitos e sem a ISO/IEC 27002, os controlos definidos no Anexo A, dificilmente são implementados por insuficiente aclaração. Numa outra perspetiva, alguns dos mapeamentos efetuados suscitam incerteza. É o caso da *Ação 5.8 — Afiliação nas comunidades nacionais e internacionais de CSIRT*, onde se alega *"Esta ação, na norma em estudo, não se relaciona com nenhum dos controlos"*. A afirmação não é verosímil, verificando-se através da metodologia definida, um elo AL, com o controlo A.6.1.4 - Contacto com grupos de interesse especial. Também a *Ação 5.1 — Nomear um CISO* é mapeada ao controlo A.16.1.1 - Responsabilidades e procedimentos (no âmbito específico da gestão de incidentes de segurança da informação), no entanto, não se infere o porquê do não mapeamento ao controlo natural A.6.1.1 - Funções e responsabilidades de segurança da informação ou mesmo ao A.6.1.2 - Segregação de funções. Fornecendo um último exemplo, a *Ação 4.3 — Análise de risco - reavaliação* é mapeada ao controlo da norma A.17.1.3 — Verificar, rever e avaliar a continuidade da segurança de informação. Ora o controlo está subordinado ao tema A.17 — Aspetos de segurança da informação na gestão da continuidade do negócio e, por conseguinte, a relação com a Ação 4.3 é desfasada. O texto da própria Ação refere a *"fase 1"*, subentendendo-se alusão com a *Ação 1.6 — Estabelecimento de metodologia de Análise de Risco*. O espírito da Ação refere-se aos requisitos (não controlos) 6.1 — Ações para endereçar riscos e oportunidades, 6.2 — Objetivos de segurança

da informação e planeamento para os alcançar, 8.2 — Avaliação de risco, 8.3 — Tratamento de risco e 10.2 — Melhoria contínua.

Este documento contribui com uma metodologia de mapeamento entre os controlos do RCMCS com os da ISO 27001. Por outro lado, peca no processo de mapeamento, que encerra algumas incongruências.

A investigação de Chamberlain designada *«Beginning the information security journey for small and medium enterprises through business continuity planning and infrastructure automation»* (Chamberlain, 2021) realiza uma revisão bibliográfica na descoberta das questões que as PME enfrentam quando implementam práticas de segurança da informação, resumindo as recomendações prevalecentes, e produzindo ensinamentos adaptáveis e acessíveis, que possam ser usados no aumento da sua resiliência, face a incidentes de segurança da informação. O autor, decorrente das suas observações, explica que as pequenas e médias empresas ignoram os seus riscos de segurança da informação, porque são difíceis de enumerar e quantificar. São enumerados os principais fatores, que reduzem o custo de uma falha de sistema, conforme o fabricante IBM[18]: (i) Teste de resposta a incidentes; (ii) Planeamento da continuidade de negócio; (iii) Treino dos colaboradores; (iv) Desenvolvimento seguro de *software*.

Este documento contribui com os principais fatores que diminuem as falhas de sistemas informáticos. Por outro lado, peca pela não existência material dos fatores enumerados.

O trabalho de Faria denominado «Gestão da Cibersegurança em empresas Transnacionais relacionadas com Transações Financeiras Críticas de espectro Macroeconómico» cria uma matriz de avaliação da cibersegurança baseada nos controlos da norma ISO/IEC 27001:2013, complementada com o mapeamento entre várias regulamentações obrigatórias e voluntárias e os requisitos exigidos, no contexto da atividade de empresas transnacionais relacionadas com transações financeiras críticas de espectro macroeconómico. O principal resultado do projeto consiste na entrega de uma matriz de avaliação para a cibersegurança, que infelizmente, presumivelmente pelo seu dimensionamento, não se encontra disponível na dissertação, tendo sido anexada. Percebe-se que o mapeamento entre a norma base ISO/IEC 27001:2013 e os restantes documentos, recai em *"mapas disponíveis na página oficial"* de cada um. Em relação ao RGPD essa indicação não é clarificada. Perscrutando a cartografia entre a ISO/IEC 27001:2013 e o RGPD detetam-se algumas desarmonias. A título de exemplo, interliga-se o requisito 7.5 — Informação documentada com o artigo

18 https://www.ibm.com/

30.º — Registos das atividades de tratamento, o que se aceita. Contudo, o controlo A.8.1.1 - Inventário de ativos é esquecido e deve estar referenciado conforme se pode constatar no artigo «IAPP-OneTrust Research: Bridging ISO 27001 to GDPR».

Este documento contribui com o mapeamento entre a ISO/IEC 27001:2013 e outras *frameworks* num setor particular de atividade económica. Por outro lado, peca na qualidade do mapeamento e ausência de entregáveis.

O artigo de Taherdoost intitulado *«Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview»* pormenoriza a importância das normas de cibersegurança, na demonstração se um sistema de informação pode satisfazer os requisitos de segurança através de uma série de melhores práticas e procedimentos. Contudo, é um desafio para as empresas adotar a norma mais apropriada com base nas suas exigências de cibersegurança. O estudo apresenta uma revisão das normas e *frameworks* de cibersegurança mais frequentemente aproveitadas, com base em documentos existentes no campo da cibersegurança e na aplicação dessas normas e *frameworks* a vários casos de uso, no intuito de ajudar as organizações a selecionar a que melhor se adequa aos seus requisitos de cibersegurança.

A metodologia recorrida na seleção final dos 17 normativos e *frameworks*, de um conjunto inicial de cerca de 250 mil documentos, é detalhada e baseou-se na pesquisa por palavras-chave específicas ao tema.

Este documento contribui com uma metodologia de pesquisa em fontes de informação e uma coleção dos normativos de segurança da informação mais implementados pelas empresas. Por outro lado, peca pela não consubstancialização de nenhum dos normativos anunciados.

2.4 SUMÁRIO

Os documentos apresentados anteriormente fraquejam, em certa medida, no prisma de não discursarem ações práticas para as PME, subentendam-se Portuguesas. Baseiam-se essencialmente nas grandes bíblias normativas e narrativas de largo espectro, indicando *o que fazer*, mas não *o como fazer*. Acalenta-se que a dissertação em causa não incorra no mesmo prejuízo. durantea investigação foi possível encontrar vários documentos mais contundentes e que estão mais alinhados com a proposta da dissertação. Não obstante tal facto, todos os trabalhos exteriorizam contributos e falhas, conforme corroborado precedentemente e sintetizado na Tabela 1 subsequente.

Tabela 1: Contributos e Omissões

Responsável	Criação	Tema	Contributo	Omissão
Alharbi et al.	«The Impact of Cybersecurity Practices on Cyberattack Damage: The Perspective of Small Enterprises in Saudi Arabia»	C	Enumeração das práticas mais eficazes de supressão de riscos cibernéticos, que as pequenas empresas devem adotar.	Falta de desdobramento das práticas em ações mensuráveis.
Chak	«Managing cybersecurity as a business risk for small and medium enterprises»	C	Três controlos de investimento módico, a serem acolhidos pelas pequenas organizações.	Imaterialização dos controlos propostos em afazeres tangíveis.
Carmo Quaresma	«Monitorização de eventos numa PME»	C	Democratização das soluções de código aberto, de custo ínfimo, face aos programas ditos comerciais.	Reduzido leque de observações efetuadas.
Cook	«Effective Cyber Security Strategies for SmallBusinesses»	C	Destrinçar de fatores eficazes face ao cibercrime.	Não ilustração dos passos necessários a assegurar essa eficácia.
Jideani	«Towards a cybersecurity framework for South African e-retail organizations»	C	Nova *framework* e estratégias de contenção relativas a ciberataques.	Supressão da materialização das estratégias.
Matos	«Cibersegurança: políticas públicas para uma cultura de cibersegurança nas empresas»	C	Diligências na concretização de uma cultura empresarial de proteção face a ciberataques.	Não trilhar o caminho efetivo no processo de disrupção cultural necessário a tal empreitada.
Nabila	«The Impact of Cyber Security on SMEs»	C	Método de procura de informação.	Apresentar um âmbito parco, resumido a duas tecnologias.
Offers	«Understanding factors influencing SME's decision makers when implementing cybersecurity measures: a protection motivation perspective»	C	Discernimento das variáveis que influenciam positiva e negativamente a concretização de medidas evasivas a ataques maliciosos.	Utilidade prática duvidosa para com as SME.
Saber	«Determining Small Business Cybersecurity Strategies to Prevent Data Breaches»	C	Identificação de quais as medidas adotadas por pequenos negócios, no combate ao cibercrime.	Incapacidade em esmiuçar quais as políticas, formações e tecnologias a adotar.
Silva Baptista	«O fator humano na cibersegurança»	C	Quadro revelador do grau de sensibilização e consciencialização em cibersegurança, que determinada função profissional requer.	Falhar em apresentar um programa com tarefas, métricas e objetivos a serem conseguidos pelas empresas.
Whitehead	«Investigation of factors influencing cybersecurity decision making in Irish SME's from a senior manager/owner perspective»	C	Coeficientes fulcrais nas decisões de investimento em cibersegurança.	Não descriminar quais os investimentos que minimizam e maximizam os coeficientes.
Zec	«Cyber security Measures in SMEs: a study of IT professionals' organizational cyber security awareness»	C	Mescla de indicadores da causa das SME encontrarem-se mais voláteis a ciberataques.	Ausência de pragmatismo.
Alvega	«Privacy awareness in Portuguese SMEs»	P	Aferição de dificuldades das PME Portuguesas na consumação do RGPD.	Afunilamento somente nas soluções de perímetro.
Ashraf	«GDPR Implementation Framework for SMEs»	P	*Framework* simplicada na busca da conformidade perante o RGPD nas SME.	Não endereçar todos os requisitos subjacentes ao Regulamento.
Carvalho Silva	«RGPD aplicado nas PME portuguesas»	P	Perceção do nível de implementação do RGPD nas PME.	descuidar em exibir uma estratégia de como empreender o Regulamento nos processos das empresas.
Fischer	«Guidelines for SME adaption to GDPR Case study of Evalent»	P	Ações práticas no cumprimento do RGPD nas SME.	Conjunto parcimonioso de entregáveis.
Mário Antunes et al.	«Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal»	S	Assimilar as dificuldades das PME em construirem um SGSI baseado em exclusivo na norma ISO/IEC 27001.	Descartar dos requisitos das secções quatro a dez e o não foco nos entregáveis.
Azinheira	«Desenvolvimento de uma metodologia para avaliação do estado da segurança informática em PME»	S	Metodologia de mapeamento entre os controlos do RCMCS com os da ISO 27001.	Processo de mapeamento, que encerra algumas incongruências.
Chamberlain	«Beginning the information security journey for small and medium enterprises through business continuity planning and infrastructure automation»	S	Principais fatores que diminuem as falhas de sistemas informáticos.	Não existência material dos fatores enumerados.
Faria entregáveis.	«Gestão da Cibersegurança em empresas Transnacionais relacionadas com Transações Financeiras Críticas de espectro Macroeconómico»	S	Mapeamento entre a ISO/IEC 27001:2013 e outras *frameworks* num setor particular de atividade económica.	Qualidade do mapeamento e ausência de
Taherdoost	«Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview»	S	Metodologia de pesquisa em fontes de informação e uma coleção dos normativos de segurança da informação mais implementados pelas empresas.	Não consubstancialização de nenhum dos normativos anunciados.

Legenda: C - Cibersegurança | P - Privacidade e Proteção de Dados Pessoais | S - Segurança da Informação

A presente dissertação pretende colmatar as falhas encontradas na literatura, através da reparação de tais omissões. Assim sendo, é auspicioso constatar, que não há bibliografia equivalente. O leitor é instigado a identificar, uma lista englobando controlos de diversas *frameworks* e de uma miríade de atributos, em concordância com as tabelas 3 e 7, centrada nas empresas nacionais.

3

METODOLOGIA

O termo metodologia significa *"estudo dos caminhos, dos instrumentos usados para se fazer ciência"* (Demo, 1995), sendo também, segundo Demo, *"disciplina instrumental ao serviço da pesquisa"* e *"visa conhecer caminhos do processo científico"*, além de desbravar *"os limites da ciência"*. A utilização de uma metodologia fornece uma abordagem sistemática à gestão de qualquer projeto, independentemente da sua natureza e objeto, assegurando que todos os aspetos associados são planeados, executados e monitorizados eficaz e consistentemente. Somente uma prática estruturada e constante, permite desconstruir um problema complexo em fragmentos manejáveis, executados coerentemente, eliminado erros e permitindo analisar resultados.

3.1 ENQUADRAMENTO E RESTRIÇÕES

A resolução do problema da construção de um manual prático sobre a segurança e privacidade da informação munido de entregáveis é o âmago da dissertação. No entanto, um desafio desta envergadura e amplitude, acarreta a existência de restrições não passíveis de resolução nos moldes e forma da presente dissertação. A balização da extensão das atividades e a introdução de novas tecnologias, pela constante evolução (disrupção) da transformação digital, obstaculizam o trabalho desenvolvido. Em relação à primeira limitação, há que focar nas atividades nucleares à materialização do manual de cibersegurança para a realidade das PME e não dispersar em detalhes ou empreitadas, que apresentem uma valorização residual face aos objetivos organizacionais, e, em contrapartida, tragam um acréscimo de trabalho não condizente com o ganho expectável. Por exemplo, remover ou reordenar as cifras fracas na versão 1.2 do protocolo *Transport Layer Security* (TLS).

No que concerne à segunda contingência, a transladação das cargas de trabalho local para a nuvem, tem proporcionado novos paradigmas de arquitetura (e.g., micro-segmentação, micro-serviços, computação sem servidor[1]), que exigem a aplicação constante de novos controlos de segurança e privacidade. Estas tecnologias, algumas embrionárias, são englobadas, no entanto, não se garante a todas o mesmo grau de

1 *Serverless computing* na designação anglo-saxónica.

detalhe, baseando o autor, as escolhas nas que melhor servem, na sua perspetiva empírica, os interesses das PME.

Há um terceiro problema merecedor de destaque. A caracterização das PME, não é objeto de uma análise meticulosa por cada setor de atividade económica em Portugal (e.g., industrias extrativas, atividades imobiliárias, transporte e armazenagem). Esta caracterização traz inegáveis mais-valias na construção de cenários, casos de uso, avaliação de risco e Análise de Impacto no Negócio (AIN)[2], que por si só, é matéria suficiente para uma nova dissertação. Tal exigirá auscultação aos associados das diversas associações empresariais espalhadas pelo país, na obtenção de uma amostra representativa de cada setor e posterior estudo dos dados recolhidos, entre outras tarefas. Assim, a caracterização é efetuada a nível macro, tendo em conta, variáveis globais transversais aos inúmeros setores, como sendo os objetivos de negócio, o pilar financeiro e o efeito reputacional.

3.2 ESBOÇO MACRO

A metodologia[3] adotada no desenlace do tema em exposição e ilustrada na Figura 1 em perspetiva geral e na Figura 14 em modo detalhado no final do capítulo, está estruturada num conjunto alargado de operações apresentadas subsequentemente.

2 *Business Impact Analysis (BIA)* na designação anglo-saxónica.

3 Nota do autor: os saberes publicados sobre estes enunciados são infindáveis, não sendo exequível, que sejam todos objeto de perquirição, no intervalo de tempo talhado para esta empreitada. Nem todas as normas, controlos e entregáveis são tidas em apreço. A alternativa seria optar por um estudo singular, mas não representativo da pluralidade rica nos domínios em observação, nem abonando tão eficazmente os resultados esperados. A triagem efetuada e ilustrada nos capítulos sequentes, é na visão do autor, a que melhor responde às exigências das PME.

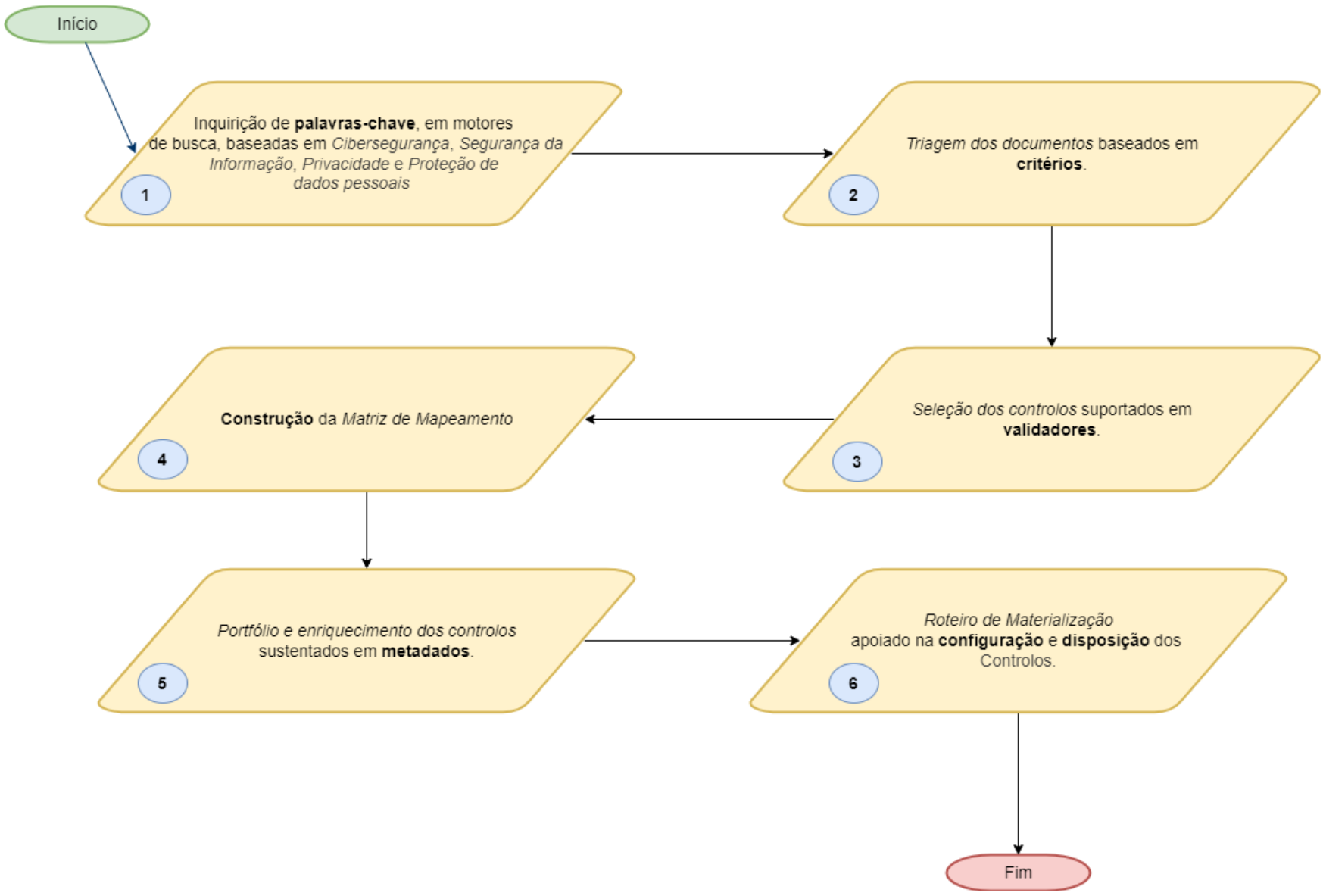


Figura 1: Metodologia Macro

Primeiramente são objeto de estudo bibliográfico, as múltiplas propostas desenhadas relativas a programas de segurança da informação, cibersegurança, privacidade e proteção de dados pessoais, disponibilizadas por agências governamentais (e.g., NIST[4], NCSC[5]) e organizações normativas (e.g., ISO[6], CSA[7]), elencando-se todos os controlos e requisitos[8] mandatórios de cada *framework*, norma internacional e regulamentação. Ulteriormente materializa-se uma matriz, que condensa e relaciona as ações de cada norma. Consecutivamente extraem-se os elementos comuns e primordiais, desconstroem-se em distintos afazeres e enumeram-se os respetivos e necessários entregáveis, sendo edificados. Consoante a dificuldade em se compreender o conceito e alcance de determinado controlo, ação e respetivo entregável, literatura adicional é objeto de estudo. Como as organizações, mesmo dentro de um qualquer setor de atividade, denotam predicados distintos em relação ao grau de aversão ao risco, cultura corporativa, objetivos estratégicos, músculo financeiro, disponibilidade e capacidade de recursos humanos, entre outros, identificam-se três tipos de perfis, sendo que cada sociedade opta por um:

- Perfil Nuclear: inclui os controlos e requisitos basilares de segurança da informação, cibersegurança, privacidade e proteção de dados pessoais, tendo o enfoco nas medidas técnicas. Aplicação de *frameworks* simplificadas circunscritas a vinte controlos e cinco requisitos. Perfil ideal para empresas com inexistente ou parca maturidade em processos, transformação digital, governança de TI, recursos humanos não alocados em exclusivo ao projeto e reduzido fluxo de caixa[9]. Corresponde ao P na sigla PME.
- Perfil Definido: inclui os controlos e requisitos cabais de segurança da informação, cibersegurança, privacidade e proteção de dados pessoais, tendo o enfoco nas medidas técnicas e fundamentos organizacionais. Aplicação de *frameworks* completas não circunscritas em número de controlos e requisitos. Perfil ideal para empresas com um conjunto de processos determinados, transformação digital e governança de TI em sintonia com a estratégia de negócio, alocação de recursos humanos em exclusivo ao projeto e fluxo de caixa saudável. Corresponde ao M na sigla PME.
- Perfil Otimizado: inclui os controlos e requisitos complementares de segurança da informação, cibersegurança, privacidade e proteção de dados pessoais,

4 https://www.nist.gov/
5 https://www.ncsc.gov.uk/
6 https://www.iso.org/home.html
7 https://cloudsecurityalliance.org/
8 Nota do autor: numa linguagem informal, um requisito diz-nos o que fazer, mas não como o fazer, e é aqui que entram os controlos (Curtis, 2020). Um requisito pode ser mitigado por vários controlos e um controlo pode mitigar vários requisitos (Diligent, 2022). No entanto, o autor relativiza esta distinção em certos trechos e ignora-a em outros. Não é de suma importância para o trabalho em apreço, cogitar e considerar esta distinção no contexto das PME.
9 *Cash Flow* na designação anglo-saxónica.

tendo o enfoco na melhoria contínua, medição e otimização das medidas técnicas e organizacionais. Aplicação de *frameworks* avançadas em Táticas, Técnicas, e Procedimentos (TTP)[10]. Perfil ideal para empresas com processos inequívocos e orientadas por dados[11], transformação digital e governança de TI evidentes com a estratégia de negócio, alocação de recursos humanos em exclusivo durante e após implementação do SGSPI e fluxo de caixa saudável. Corresponde ao E na sigla PME.

Todas as empresas devem almejar conformidade categórica com o perfil Nuclear. Este patamar granjeia uma proteção adequada contra atores maliciosos, utilizando técnicas de intrusão primitivas em complexidade e esforço empregue, focando-se em vulnerabilidades amplamente documentadas na *internet*. Sob outra perspetiva, empresas com exposição acentuada em canais de comunicação tradicionais e digitais, que tratam de dados pessoais nomeadamente de terceiros em volume considerável, realizem transações financeiras em escala apreciável, ou processem operações de negócio envoltas em segredo industrial e comercial, devem optar pelo perfil Definido.

Cibercriminosos organizados (LookingGlass, s.d.) gravitam em torno deste alinhamento, desenvolvendo programas de computador maliciosos[12] (e.g., *phishing*, *ransomware*, cavalo de troia[13]), num lacónico espaço temporal, explorando deficiências e fraquezas das aplicações, com o intuito de extorquir e chantagear. Oferecendo proteção em oposição a atores patrocinados por Estados, acompanha-nos o perfil Otimizado.

Estes malfeitores estão munidos de recursos técnicos, financeiros e materiais sem paralelo, sendo necessário assegurar controlos resilientes, escaláveis e múltiplas camadas defensivas. Organizações outorgando valor nas áreas militares, infraestruturas críticas (e.g., energia, barragens), setor financeiro, serviços de emergência (e.g., forças polícias, INEM), enquadram-se neste nível.

As organizações ao terem requisitos regulamentares, legislativos e de conformidade específicos, bem como, ativos tecnológicos e de informação únicos, devem avaliar cuidadosamente os riscos de negócio e as suas características intrínsecas e precisar qual o perfil apropriado. Cumpre explanar a liberdade de se poder optar por uma mescla dos vários perfis, desde que se garanta as premissas do nível Nuclear. Assim como, a ordem pela qual os controlos e requisitos são relatados, não obriga à sua

10 *Tactics, Techniques, and Procedures* na designação anglo-saxónica.
11 *Data-driven* na designação anglo-saxónica.
12 *Malware* na designação anglo-saxónica.
13 *Trojan* na designação anglo-saxónica.

execução sequencial, podendo ser materializados pelo critério que o leitor assim melhor entender.

Seguindo a ordem planeada, evitar-se-á, à partida, potenciais incongruências, como, por exemplo, não salvaguardar o comprometimento da gestão de topo na alocação dos recursos humanos e financeiros necessários a tal demanda. No entanto, há a realçar, que um negócio em conformidade[14] não é congénere a um negócio seguro.

E, não obstante, a conformidade continua a servir de bitola nos contratos comerciais. Liderar o negócio, favorecendo a tecnologia e os comportamentos que diminuem o risco e aumentem a segurança, deve ser o objetivo. A questão não pode assentar no que é exigido realizar para asseverar a conformidade da empresa. O foco deve ser a forma como desenvolver as atividades do trabalho diário, na procura de as tornar o mais seguras possível. Em epítome, o foco tem de se centrar nas atividades empresariais, nas pessoas que as realizam e no esforço empregue em subtrair a complexidade das mesmas, adicionar etapas de garantia de segurança, aplicar barreiras de proteção no suporte à consistência e colocar redes de segurança para limitar erros (Johnson, 2022).

3.3 ANÁLISE DETALHADA

Tal como um escritor arguto aplica um conjunto diversificado de técnicas e ferramentas na exposição de uma narrativa mais criativa e entusiasmante, a conciliação de plurais *frameworks* nas temáticas em estudo, permite obter um programa mais completo, robusto e resiliente. Ingressemos no relato minucioso do método[15] empregue:

14 *Compliant business* na designação anglo-saxónica.

15 O autor segue a metodologia qualitativa, aplicando uma panóplia de técnicas de recolha de informação essencialmente descritiva (e.g., transcrições de entrevistas provenientes da pesquisa efetuada no Capítulo 2, documentos pessoais, artigos científicos, dissertações académicas, *frameworks*, normativos, observações de outros profissionais), para agregar dados qualitativos, executando uma arguição indutiva. Partindo de experiências e análises sobre factos particulares no Capítulo 4 e Capítulo 5, inferem-se conclusões gerais, relatadas no Capítulo 6. Não existe a preocupação em se avaliar empiricamente quaisquer hipóteses. O produto final do estudo, ganha forma à medida que os dados vão sendo explorados, não se conhecendo de antemão qual é a sua forma ou conteúdo (Patton, 2015; Pesce, 2009; Pinto et al., 2018). Adicionalmente, peritos em investigação, afirmam que a utilização de múltiplas fontes, aumenta a confiabilidade dos dados e significativamente comprova os dados emergentes (Marshall et al., 2021; Morse e McEvoy, 2014).

3.3.1 *Seleção e Pesquisa de Vocábulos Relacionados*

Primeiramente digitam-se cadeias de texto singulares em motores de busca da *internet* e bases de dados especializadas[16]:

i *CERT*[17] *Critical Controls*;

ii *Critical Security Controls*;

iii *Cybersecurity SME*[18] *Controls*;

iv *Cybersecurity Strategy for SME*;

v *Cybersecurity Small Business Guide*;

vi *Essential controls for SME*;

vii *Common Cybersecurity Frameworks*;

viii *Information Security Controls*;

ix *Baseline cyber security controls*;

x *SME IT Security*;

xi *Small Medium Enterprises IT security*;

xii *Small Medium Business IT security*;

xiii *GDPR*[19] *compliance*;

xiv *GDPR implementation*;

xv *GDPR guidelines*;

xvi *GDPR framework*.

3.3.2 *Triagem dos Resultados Obtidos*

Ao longo do segundo momento, depuram-se as decorrências precedentemente granjeadas, aplicando os posteriores critérios:

16 https://www.mdpi.com/; https://www.sciencedirect.com/; https://www.standict.eu/standards-repository

17 Nota do autor: uma panóplia de acrónimos análogos são englobados nas buscas, nomeadamente CSIRT, CSIRC, CIRC, CIRT, IHT, IRC, IRT, SERT, SIRT. (Ruefle, 2007)

18 Nota do autor: adicionalmente o acrónimo SMB também é tido em conta nas procuras.

19 Nota do autor: ademais o acrónimo RGPD é abrangido.

i Origem dos textos baseada em entidades plausíveis e profissionais do setor certificados[20], i.e., agências governamentais (e.g., DHS[21]), redes CSIRT[22], bibliotecas académicas[23], centros de cibersegurança[24], associações profissionais de TI (e.g., IAPP[25], ISACA[26]) e organizações de padrões técnicos (e.g., CEN[27]);

ii Escrita em idioma português ou inglês;

iii Leitura do título e resumo (*abastract*), observando o seu enquadramento nos resultados esperados;

iv Optar pela versão mais recente do documento ou por uma não obsoleta;

v Aplicável a todas as organizações, independentemente do tipo, tamanho, natureza ou do setor;

vi Eleger controlos e requisitos pragmáticos, prescritivos, concretos e tecnologicamente neutros, com nula ou efémera margem para alegações;

vii Exequível com recursos humanos internos à organização ou com auxílio do prestador de TI vigente;

viii Expensa e afinco parcos na implementação das medidas;

ix Eliminação de conteúdos idênticos.

3.3.3 *Validação do Processo Cartográfico*

A palavra taxonomia é originária das palavras gregas $\tau\alpha\xi\iota\varsigma$ — arranjo ou ordem e $\nu o\mu\iota\alpha$ — método. Em termos de sistemas de informação, as taxonomias mais não são do que *"agrupamentos de dimensões e características derivadas conceptual ou empiricamente"* (Oberländer e Rau, 2019). Por outras palavras, a taxonomia refere-se à forma como classificamos hierarquicamente ou em categorias um conjunto de características comuns, ou mesmo quaisquer conceitos de conhecimento. Durante o processo desta etapa, mapeia-se a amálgama de documentos resultantes da fase anterior. A qualidade do mapeamento é fulcral. Os controlos e requisitos das cláusulas

20 Nota do autor: especialistas detentores de títulos internacionalmente reconhecidos e requisitados nos anúncios de recrutamento, como, por exemplo, *Certified Information Security Manager* (CISM) e *Certified Information Privacy Technologist* (CIPT).
21 https://www.dhs.gov/
22 E.g., https://www.redecsirt.pt/, https://www.cert.govt.nz/
23 E.g., https://fordham.libguides.com/Cybersecurity/GeneralResources
24 E.g., https://www.cncs.gov.pt/
25 https://iapp.org/
26 https://www.isaca.org/
27 https://www.cencenelec.eu/

do documento origem, devem mapear com precisão nos controlos e requisitos das cláusulas do documento destino. De outro modo, a origem pode potencialmente exceder ou ser insuficiente perante a outra parte e consequentemente resultar num desvio de eficácia ou fraqueza sob o mapeamento do controlo ou requisito (Eramba, s.d.). A forma de garantir a virtude do processo cartográfico é assegurado pelos quatro seguintes validadores:

- Tríade CIA[28]: as cláusulas do documento origem e as cláusulas do documento destino circunscrevem as mesmas propriedades da tríade CIA. Em caso afirmativo prossegue-se para o próximo validador. Em caso negativo, o mapeamento é descartado para o controlo ou requisito em análise;
- Domínio, Função e Tipo: captura de correspondência entre os atributos do controlo ou requisito de origem e os de destino. São perscrutados os domínios explanados na obra *Security and Privacy Controls for Information Systems and Organizations* da NIST, as funções "preventivo", "detetivo" e "corretivo", e os tipos "físico", "técnico" e "administrativo". Em caso afirmativo prossegue-se para o próximo validador. Em caso negativo, o mapeamento é descartado para o controlo ou requisito em análise.
- Valor Semântico: o conteúdo informativo das cláusulas dos documentos origem e destino carecem do mesmo significado. A partir da decomposição do significado dos clausulados que compreendem o controlo ou requisito de origem a mapear no destino, apurar se existe o mesmo sentido, no que concerne às relações de equivalência (sinonímia), oposição (antonímia), relações parte — todo/todo — parte (meronímia/holonímia) e hierárquicas (hiperonímia/hiponímia) (Lopes e Rio-Torto, 2007). Em caso afirmativo prossegue-se para o próximo validador. Em caso negativo, o mapeamento é descartado para o controlo ou requisito em análise;
- Conformidade de Mapeamento: cada controlo ou requisito de origem e destino é constituído por uma ou mais ações, que ao serem executadas, garantem a conformidade com o objetivo delineado para esse mesmo controlo ou requisito. A sobreposição do conjunto de ações proveniente do clausulado de origem sob

28 Nota do autor: as propriedades (C) confidencialidade, (I) integridade e (A) disponibilidade são um dos pilares fundamentais de segurança da informação (Young, s.d.). Existem variações mais complexas, como a introduzida por Parker no seu livro *Fighting computer crime*, que além da tríade CIA, admite três princípios adicionais *Possesion* ou *Control*, *Authenticity* e *Utility*. Embora seja considerado por alguns especialistas um modelo mais completo, para o contexto em causa, não justifica os acréscimos de corroborações a efetuar. Não obstante, o leitor está incentivado a permutar este ou outro(s) validador(es), caso vislumbre benefícios suplementares.

o clausulado de destino, levanta as várias hipóteses quantificadas na Figura 2 e esplanadas subsequentemente:

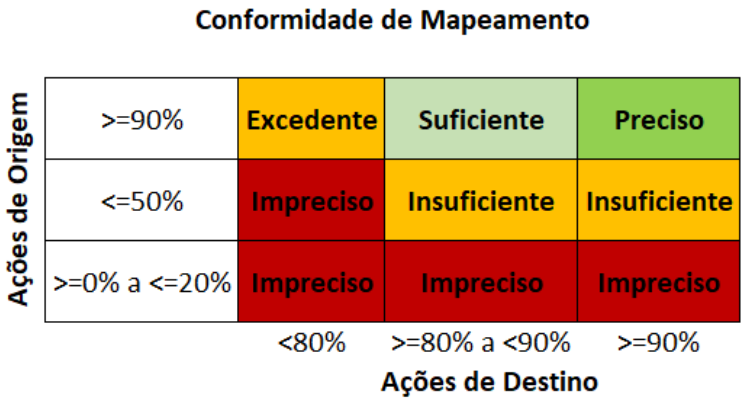


Figura 2: Conformidade de Mapeamento

– Se as ações do controlo ou requisito de origem, estão na totalidade ou maioritariamente mapeadas nas do destino e as ações do requisito de destino, não têm ou praticamente não têm ações adicionais em relação às pedidas pela origem, então estamos perante uma Conformidade do Mapeamento essencialmente Precisa (Figura 3). Mapeamento é efetuado;

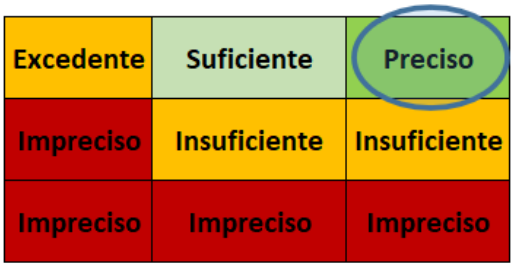


Figura 3: Conformidade de Mapeamento Preciso

– Se as ações do controlo ou requisito de origem, estão na totalidade ou maioritariamente mapeadas nas do destino e as ações do requisito de destino, têm relativamente mais ou menos ações adicionais em relação às pedidas pela origem, então estamos perante uma Conformidade de Mapeamento razoavelmente Precisa (Figura 4). Mapeamento é efetuado;

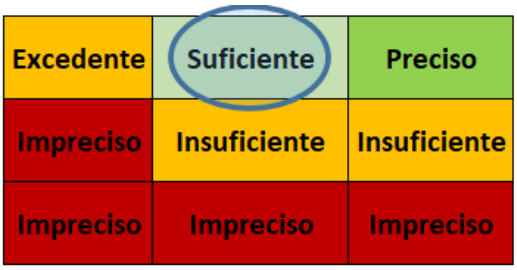


Figura 4: Conformidade de Mapeamento Suficiente

– Se as ações do controlo ou requisito de origem, estão na totalidade ou maioritariamente mapeadas nas do destino e as ações do requisito de destino, têm inegavelmente mais ações adicionais em relação às pedidas pela origem, então estamos perante uma Conformidade de Mapeamento onde o destino excede a origem (Figura 5). Mapeamento não é efetuado;

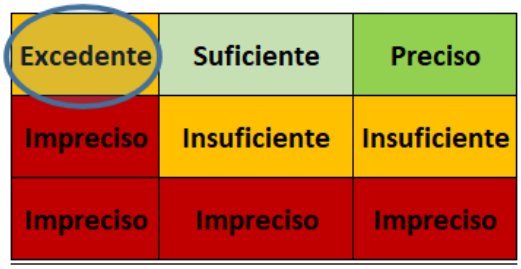


Figura 5: Conformidade de Mapeamento Excedente

– Se as ações do controlo ou requisito de origem, não estão mapeadas até metade nas do destino e as ações do requisito de destino, não têm ou praticamente não têm ações adicionais em relação às pedidas pela origem, então estamos perante uma Conformidade do Mapeamento potencialmente insuficiente no destino (Figura 6). Mapeamento não é efetuado;

Figura 6: Conformidade de Mapeamento Insuficiente

– Se as ações do controlo ou requisito de origem, não estão mapeadas até metade nas do destino e as ações do requisito de destino, têm relativamente mais ou menos ações adicionais em relação às pedidas pela origem,

então estamos perante uma Conformidade do Mapeamento potencialmente insuficiente no destino (Figura 7). Mapeamento não é efetuado;

Figura 7: Conformidade de Mapeamento Insuficiente

– Se as ações do controlo ou requisito de origem, não estão mapeadas até metade nas do destino e as ações do requisito de destino, têm inegavelmente mais ações adicionais em relação às pedidas pela origem, então estamos perante uma Conformidade do Mapeamento questionável (Figura 8). Mapeamento não é efetuado;

Figura 8: Conformidade de Mapeamento Impreciso

– Se as ações do controlo ou requisito de origem, não estão ou maioritariamente não estão mapeadas nas do destino e as ações do requisito de destino, não têm ou praticamente não têm ações adicionais em relação às pedidas pela origem, então estamos perante uma Conformidade do Mapeamento não Precisa (Figura 9). Mapeamento não é efetuado;

Figura 9: Conformidade de Mapeamento Impreciso

– Se as ações do controlo ou requisito de origem, não estão ou maioritariamente não estão mapeadas nas do destino e as ações do requisito de destino, têm relativamente mais ou menos ações adicionais em relação às pedidas pela origem, então estamos perante uma Conformidade do Mapeamento não Precisa (Figura 10). Mapeamento não é efetuado;

Figura 10: Conformidade de Mapeamento Impreciso

– Se as ações do controlo ou requisito de origem, não estão ou maioritariamente não estão mapeadas nas do destino e as ações do requisito de destino, têm inegavelmente mais ações adicionais em relação às pedidas pela origem, então estamos perante uma Conformidade do Mapeamento não Precisa (Figura 11). Mapeamento não é efetuado.

Figura 11: Conformidade de Mapeamento Impreciso

No caso do *Mapeamento não é efetuado* dá origem a num novo controlo.

3.3.4 *Definição da Matriz de Mapeamento*

Para a primeira *framework* selecionada não há termo de comparação, sendo cartografada na íntegra. As restantes são alvo do crivo dos validadores supraditos, num relacionamento um-para-muitos (1:N), conforme a Figura 12.

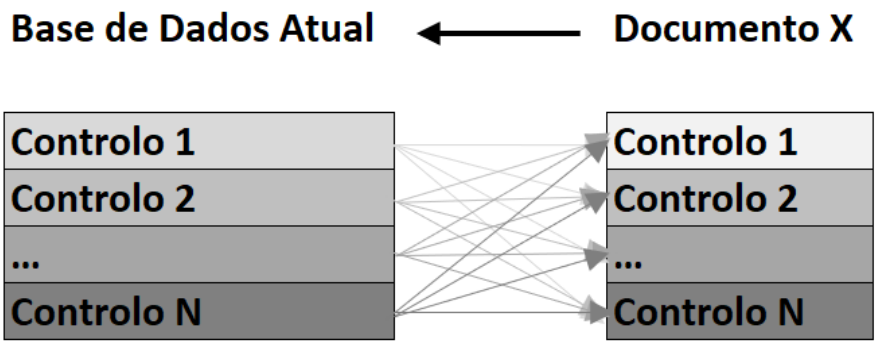


Figura 12: Introdução de Novo Documento

A tabela sequente apelidada *Modelo da Matriz de Mapeamento*, verte a disposição do pretendido, concatenando as ações das difusas *frameworks*, padrões e regulamentos sob reflexão.

Tabela 2: Modelo da Matriz de Mapeamento

#	**Nome do Controlo**	**F \P \R 1**	**F \P \R 2**	**...**	**F \P \R N**
1	NC_1	FPR_1	FPR_2	...	FPR_N
2	NC_2	FPR_1	FPR_2	...	FPR_N
...	...	...	...	...	FPR_N
N	NC_N	FPR_1	FPR_2	...	FPR_N

Legenda: F - *Framework* | P - Padrão | R - Regulamento

3.3.5 *Portfólio de Controlos*

Construção das ações, entregáveis e demais atributos de cada controlo, alicerçados na Matriz de Mapeamento. Estamos perante um processo de enriquecimento dos controlos, por um conjunto diverso de metadados holísticos apresentados na Tabela 3 e intrínsecos na Tabela 7, acrescentado significado e razão à necessidade de implementação de cada um.

3.3.5.1 *Metadados Holísticos*

Tabela 3: Modelo do Portfólio de Controlos com Metadados Holísticos

Identificador	Nome	Objetivo	Racionalidade		Tipo			Função			Prop			Do	MMC					Ref
[v<VER>].<DO>.<CT>.[<AC>]	[A-Za-z]	[A-Za-z]	Riscos {1..3}	Ameaças {1..3}	F	T	A	P	D	C	C	I	A	{20}	CA	*Ad hoc*	PER	E	AP	{0,1,2...N}

Legenda: VER - Versão | DO - Domínio | CT - Controlo | AC - Ação | F - Físico | T - Técnico | A - Administrativo | P - Preventivo | D - Detetivo | C - Corretivo | CA - Caótico | PER - Permissivo | E - Elaborado | AP - Aperfeiçoado | Prop - Propriedades | Do - Domínios | Ref - Referências

1. Identificador do controlo: todo o controlo tem um identificador no formato [v<versão>].<domínio>.<controlo>.[<ação>], onde cada elemento é um número natural {1,2...N}. Os domínios são compostos por um ou mais controlos. Um controlo é estabelecido por uma ou mais ações. Cada ação pertence a um só controlo. A etiqueta "versão" é facultativa e, caso não seja mencionada, refere-se sempre à última versão da dissertação. Uso de identificadores noutras publicações devem incluir o elemento versão. O membro "ação" é utilizado aquando da referência específica a essa componente do controlo.
2. Nome do controlo: nome da medida que modifica o risco (Garfinkel, 2015).
3. Objetivo do controlo: um conjunto de declarações de determinação, que exprimem o desejado resultado para a avaliação de um controlo de segurança (ou privacidade), ou a melhoria de um controlo (Dempsey et al., 2011).
4. Racionalidade do controlo: somatório dos riscos mitigados e das ameaças prevenidas. Por razões de assingelamento, os riscos e ameaças elencadas são no melhor três, adicionando-se a representação (...), significando a perspectiva de existir outros mais.

    a) Riscos mitigados pelo controlo: o nível de impacto potencial nas operações de uma organização (incluindo missão, funções, imagem, ou reputação), ativos da organização, ou indivíduos de uma ameaça, ou uma dada *likelihood*[29] de que essa ameaça ocorra (Ferraiolo et al., 2015).
    A escolha dos riscos tem por filosofia os sistemas de informação e não outras linhas orientadoras como a macroeconomia, onde é expectável considerar perigos, tais como, o descontrolo crónico da política orçamental ou a nefasta burocracia dos serviços públicos no caso português. Assim, e tendo em consideração os exemplos anunciados na *ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management*, afiguram-se no apêndice A uma lista de riscos.

    b) Ameaças prevenidas pelo controlo: qualquer circunstância ou evento com potencial para ter um impacto adverso nas operações organizacionais (incluindo missão, funções, imagem, ou reputação), ativos organizacionais, indivíduos, outras organizações, ou a Nação através de um sistema de informação via acesso não autorizado, destruição, divulgação, modificação

29 Nota do autor: de modo erróneo o vocábulo *likelihood* é traduzido para o termo *probabilidade* em português. A probabilidade está ligada a possíveis resultados mutuamente exclusivos e exaustivos, somando sempre um. Por seu lado, o termo *likelihood* está conectado a hipóteses, que ao contrário de resultados, não são mutualmente exclusivas ou exaustivas, não existindo limite à sua construção (Gallistel, 2015).

de informação, e/ou negação de serviço (Paulsen e Toth, 2016).
O apêndice B cataloga um resumo das ameaças elementares adaptadas da lista proveniente do *Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)* (BSI, 2018).

5. Tipo de controlo: tipificação em físico, técnico ou administrativo (Tipton e Krause, 2007).

   - Controlos Físicos: uso de medidas tangíveis (e.g., alarmes, fechaduras, identificadores pessoais), para ter sob domínio, o acesso a dispositivos eletrónicos e restantes infraestruturas físicas (e.g., armários, salas de equipamentos, escritórios) e garantir a sua proteção e respetivos conteúdos face a roubo, furto, espionagem, dano ou destruição (in)tencional (e.g., desastre natural).
   - Controlos Técnicos: aplicação de proteções embebidas ou incorporadas em dispositivos, ou comunicações físicas, aplicações e restante *software*. Também referidos como lógicos ou tecnológicos.
   - Controlos Administrativos: gestão de restrições, procedimentos operacionais e de responsabilização, e estabelecimento de medidas suplementares, incluindo autorização e habilitação, por forma a garantir um nível aceitável de proteção e acesso, aos recursos de computação. Também referidos como organizacionais, pessoa(i)s, psicológicos ou políticas.

   Na ocorrência de controlos com ações, que recaiam em mais de uma tipologia, o tipo de controlo selecionado, é o representado pelo maior número de casos. Nos cenários de igualdade ou indecisão, uma solução, é a separação de uma das tipologias num novo controlo. Outra solução, é se optar por um dos praticáveis tipos e manter a congruência, ao longo do diagnóstico aos controlos restantes. Materializando o conceito na tabela sequente, existem três ações, sendo uma do tipo "Administrativo" e duas da tipologia "Técnica". Nesta situação, o controlo de nome *Conduzir Negócios Online de Modo mais Seguro* é etiquetado de "Técnico".

Tabela 4: Tipologia das Ações no Controlo Conduzir Negócios *Online* de Modo mais Seguro

ID	Nome	Item	Ações	TdC
1.14.58	Conduzir Negócios *Online* de Modo mais Seguro	1	Transações de negócio, comerciais e bancárias em linha, apenas se devem realizar utilizando uma ligação segura.	A
		2	Apagar regularmente a *cache* do navegador *web*, ficheiros temporários da *internet*, *cookies*, e histórico.	T
		3	Ter um computador dedicado, usado somente para transações bancárias, desligado quando não necessário.	T

Legenda: ID - Identificador | TdC - Tipo de Controlo | A - Administrativo | T - Técnico

6. Função do controlo: diferenciação em preventivo, detetivo (Louisville, s.d.; Tipton e Krause, 2007) e corretivo (Abade, 2018; Garcia, 2017; Isabel Martins, 2013; Monteiro, 2015).

    - Controlos Preventivos: são os que tentam ou impedem a ocorrência de factos indesejáveis, apresentando por vezes um carácter inibidor. Também conhecidos por controlos *à priori* e proativos. Incorpora as funções Identificar e Proteger da NIST (Curtis, 2020; JTC1/SC27, 2022b).
    - Controlos Detetivos: têm como função a deteção ou correção e evidenciação (resposta) de acontecimentos não desejáveis já ocorridos. Também conhecidos por controlos *à posteriori*. Incorpora a função Detetar da NIST.
    - Controlos Corretivos: aqueles que como missão têm a retificação (recuperação) de adversidades observadas. São normalmente postos em prática após uma investigação da causa raiz (Reciprocity, 2022). Incorpora as funções Responder e Recuperar da NIST.

    A Figura 13 é um compêndio exemplificativo da harmonização dos tipos e funções de controlos (Beborta, 2021; Center, s.d.; Oliveira, 2014; Walkowski, 2019).

		Função do Controlo		
		Preventivo	Detetivo	Corretivo
Tipo do Controlo	Físico	Vedações; portões; fechaduras; porteiros e vigilantes; controlos biométricos em portas.	Circuitos fechados de televisão; registos de câmaras de vigilância; alarmes térmicos ou de movimento; inspeções à infraestrutura física.	Reparar dano físico; segunda via de um cartão de acesso.
	Técnico	*Firewall* ; sistema de prevenção de intrusão; *software* antivírus; autenticação multifator; criptografia; rede privada virtual; sistemas de prevenção de perda de dados;rede virtual local; lista de controlo de acesso.	Sistema de deteção de intrusão; honeypots; software de auditoria.	Atualizar um sistema; terminar um processo; reiniciar um sistema; colocar em quarentena um vírus; salvaguardas para recuperação posterior a um incidente.
	Administrativo	Classificação da informação; segregação de funções; políticas de contratação e terminação; sensibilização e treino dos colaboradores; plano de continuidade do negócio; aprovações, autorizações e verificações; contagem de inventários.	Rever direitos de acesso; pesquisar registos de eventos; analisar alterações não autorizadas; auditorias a processos; listas de verificação de conformidade; inventário físico; reconciliações entre diferentes conjuntos de dados.	Execução do plano de continuidade do negócio ou do plano de resposta a incidentes; ativação de seguro após roubo/furto de ativos; atualização de políticas e procedimentos após identificação de falhas num processo. Ações disciplinares.

Figura 13: Tipo e Função do Controlo

7. Propriedades do Controlo[30]: elementos da tríade CIA (JTC1/SC27, 2018a).

    - Confidencialidade: propriedade de a informação não ser disponibilizada ou divulgada a indivíduos, entidades, ou processos não autorizados.
    - Integridade: propriedade de exatidão e completude.
    - Disponibilidade: propriedade de ser acessível e utilizável a pedido por uma entidade autorizada.

8. Domínios: representa uma coleção de controlos de segurança e privacidade interligados sob a mesma temática ilustrados na Tabela 5. A nomenclatura de cada família de controlos está baseada na quinta revisão da NIST SP 800-53 (Force, 2020).

30 Nota do autor: aplicação das propriedades tem na sua génese a consideração meramente dos elementos elementares. Dando o exemplo da ameaça "fogo", a propriedade fundamental é a A. É óbvido que o fogo ao danificar um dispositivo amovível com informação armazenada alterará a propriedade I. No entanto, estamos perante um efeito do elemento primordial.

Tabela 5: Coleção de Controlos de Segurança e Privacidade

#	**Família de Controlos**	**Descrição**
1	Aquisição de Sistemas e Serviços	Focar em controlos de segurança respeitante à aquisição de sistemas e serviços. Incluem-se controlos que governam o desenvolvimento de sistemas, para assegurar que os sistemas e serviços estão conforme os padrões de segurança.
2	Auditoria e Responsabilização	Asseverar que os eventos são devidamente registados e auditados.
3	Avaliação de Risco	Identificar riscos relacionados com a organização e ativos.
4	Avaliação, Autorização e Monitorização	Garantir que os controlos de segurança e privacidade são eficazes e continuam a sê-lo ao longo do tempo.
5	Controlo de Acessos	Proteger a informação das partes interessadas contra acesso não autorizado e indevido.
6	Gestão das Configurações	Promover que os sistemas estão devidamente configurados e que as alterações são feitas de uma forma controlada e consistente.
7	Gestão do Programa	Gerir os programas de cibersegurança e privacidade.
8	Gestão do Risco da Cadeia de Fornecimento	Mitigar riscos na cadeia de fornecimento pela inclusão de políticas procedimentos.
9	Identificação e Autenticação	Preservar as identidades dos utilizadores e sistemas.
10	Integridade da Informação e Sistemas	Contribuir para a salvaguarda dos ativos da organização e reduzir o risco de violações de segurança e falhas do sistema de comunicação.
11	Manutenção	Englobar todos os aspetos da manutenção do sistema, tais como, atualizações de programas, registos, e ferramentas de inspeção.
12	Planeamento	Certificar que os planos de segurança e privacidade estão alinhados com os objetivos organizacionais, requisitos de segurança e tolerância aos riscos. Por outro lado, assegurar que os planos abordem os riscos identificados e que são regularmente revistos e atualizados.
13	Planeamento de Contingência	Preparar as organizações para responder a disrupções e minimizar impactos nas operações.
14	Proteção de Sistemas e Comunicações	Amparar as fronteiras de um sistema e assegurar que os dispositivos que funcionam em conjunto são geridos com segurança.
15	Proteção dos Suportes de Armazenamento	Cobrir como os suportes e ficheiros são utilizados, armazenados e destruídos em segurança.
16	Proteção Física e Ambiental	Defender todo o tipo de infraestruturas e localizações físicas.
17	Resposta a Incidentes	Minimizar o impacto e prevenir a ocorrência de futuros incidentes.
18	Segurança do Pessoal	Governar as pessoas através de diferentes políticas e procedimentos.
19	Sensibilização, Consciencialização e Formação	Assegurar que os utilizadores de sistemas de informação estão devidamente habilitados à sua utilização.
20	Tratamento de Dados Pessoais e Transparência	Resguardar dados sensíveis, colocando a ênfase na privacidade e no consentimento.

9. MMC[31]: aplica-se um modelo com cinco níveis de maturidade na caracterização do processo de melhoria contínua de cada controlo na organização (CMMI Product Team, 2010). O nível por omissão é o "Caótico".

Tabela 6: Modelo de Maturidade em Capacitação

Nível de Maturidade	**Condição Prática**
Caótico	Até um quinto das ações do controlo estão implementadas.
Ad hoc	Até dois quintos das ações do controlo estão implementadas.
Permissivo	Até três quintos das ações do controlo estão implementadas.
Elaborado	Até quatro quintos das ações do controlo estão implementadas.
Aperfeiçoado	Todas as ações do controlo estão implementadas.

10. Referências: sustentáculo bibliográfico à elaboração do controlo. Um controlo pode ter {0,1,2...N} referências.

3.3.5.2 *Metadados Intrínsecos*

Subsequentemente deslinda-se cada um dos controlos através dos metadados intrínsecos retratados na tabela posterior.

Tabela 7: Modelo do Portfólio de Controlos com Metadados Intrínsecos

Identificador	Nome	Item	Ações	OdA			Métricas	Perfil			E	Realizado			
[v<VER>].<DO>.<CT>.[<AC>]	[A-Za-z]	{1..N}	[A-Za-z]	A	C	R	{1,2...N}	N	D	O	[A-Za-z]	N	S	EP	I

Legenda: VER - Versão | DO- Domínio | CT - Controlo | AC - Ação | A - Alternativa | C - Complemento | R - Recomendado | N - Nuclear | D - Definido | O - Otimizado | N - Não | S - Sim | EP - Em Progresso | I - Inaplicável | OdA - Opções das Ações | E - Entregáveis

1. Identificador do Controlo e Nome do Controlo: aclarados aquando da descrição dos atributos da tabela 3.
2. Item: número da ação.
3. Ações do Controlo: caracteriza os afazeres do controlo. Unicamente a plena completude dos afazeres, traduz a mitigação efetiva das ameaças e riscos subjacentes.
4. Opções das Ações: recaem em três possibilidades. A primeira "Alternativa" permite optar entre duas ou mais ações, que possuem o mesmo objetivo, sendo conseguido por meios diferentes, à partida, não compatíveis. A segunda "Complemento" é quando existem duas ou mais ações que se completam, sendo alvitrado a execução de ambas, no entanto, a concretização de somente uma perfaz o intento. A terceira "Recomendado" significa que a prática da ação é aconselhável, mas não obrigatória.
5. Métricas: critérios de medição para determinar o desempenho de um controlo, constituído por {1,2...N} métricas ou indicadores. Embora todos os indicadores-

31 *Capability Maturity Model* na designação anglo-saxónica.

chave de desempenho[32] sejam métricas e uma parte significativa das métricas não o seja (Savkin, 2017), para o trabalho em apreço a distinção entre ambos os conceitos não é de suma importância. Como disse o estrategista militar Sun Tzu (Tzu, 2020), o general que efetua mais cálculos antes do início da batalha ganha. Isto posto, um número ou uma derivação qualitativa de um objetivo é afim neste trabalho. Valoroso é que meça.

6. Perfil: a descrição dos vários perfis já tinham sido objeto de relato, sendo agora resumidos com recurso ao instrumento visual da Tabela 8. Cada ação de um controlo mapeia sempre num único perfil.

Tabela 8: Perfil

Interrogações de Seleção	**Perfil**		
	Nuclear	*Definido*	*Optimizado*
Processos documentados com indicadores de desempenho?	{0..1}	{2..5}	{6..N}
Governança corporativa, gestão de riscos e práticas de auditoria e controle implementadas?	Nulo	Dias prévios e durante as auditorias	Parte das operações diárias
Alocação de recursos humanos à fase de projeto e posterior melhoria contínua?	Tempo parcial durante e após projeto	Exclusivo durante e parcial após projeto	Exclusivo durante e após projeto
Fluxo de caixa saudável?	Reduzido	Equilibrado	Lucrativo
Tipologia de *frameworks* aplicadas?	±{1..20} controlos e ±{1..5} requisitos	Sem limite de controlos e requisitos	Sem limite de controlos, requisitos e complexidade

7. Entregáveis do controlo: inclui qualquer processo, política, prática, ferramenta, observação ou outro conteúdo elementar ao cumprimento do controlo.

8. Realizado: estado da ação. As possibilidades estão balizadas a quatro: “Não”, “Sim”, “Em Progresso”, “Inaplicável”. O estado inicial é o “Não”. Nas situações onde haja *Opções das Ações* não empreendidas, adota-se a etiqueta “Inaplicável”.

32 Key Performance Indicator *na designação anglo-saxónica.*

3.3.6 *Roteiro de Materialização*

Aprimoração, composição e disposição dos controlos pela ordem de efetivação sugerida, tendo por base a lógica de encandeamento e harmonização ao tecido empresarial português. Apesar de a indicação do autor ser ativamente aconselhável, o leitor executa parcialmente ou na plenitude as ações de cada controlo, pela disposição que melhor sirva os objetivos estratégicos a alcançar pela organização. Primordial, mesmo, é se efetivar a materialização das ações propostas, nomeadamente as do perfil nuclear, independentemente da forma utilizada na persecução de tal demanda. As ações são objeto de ajustamento, sempre que haja incongruências, e de possível melhoramento no compêndio das mesmas.

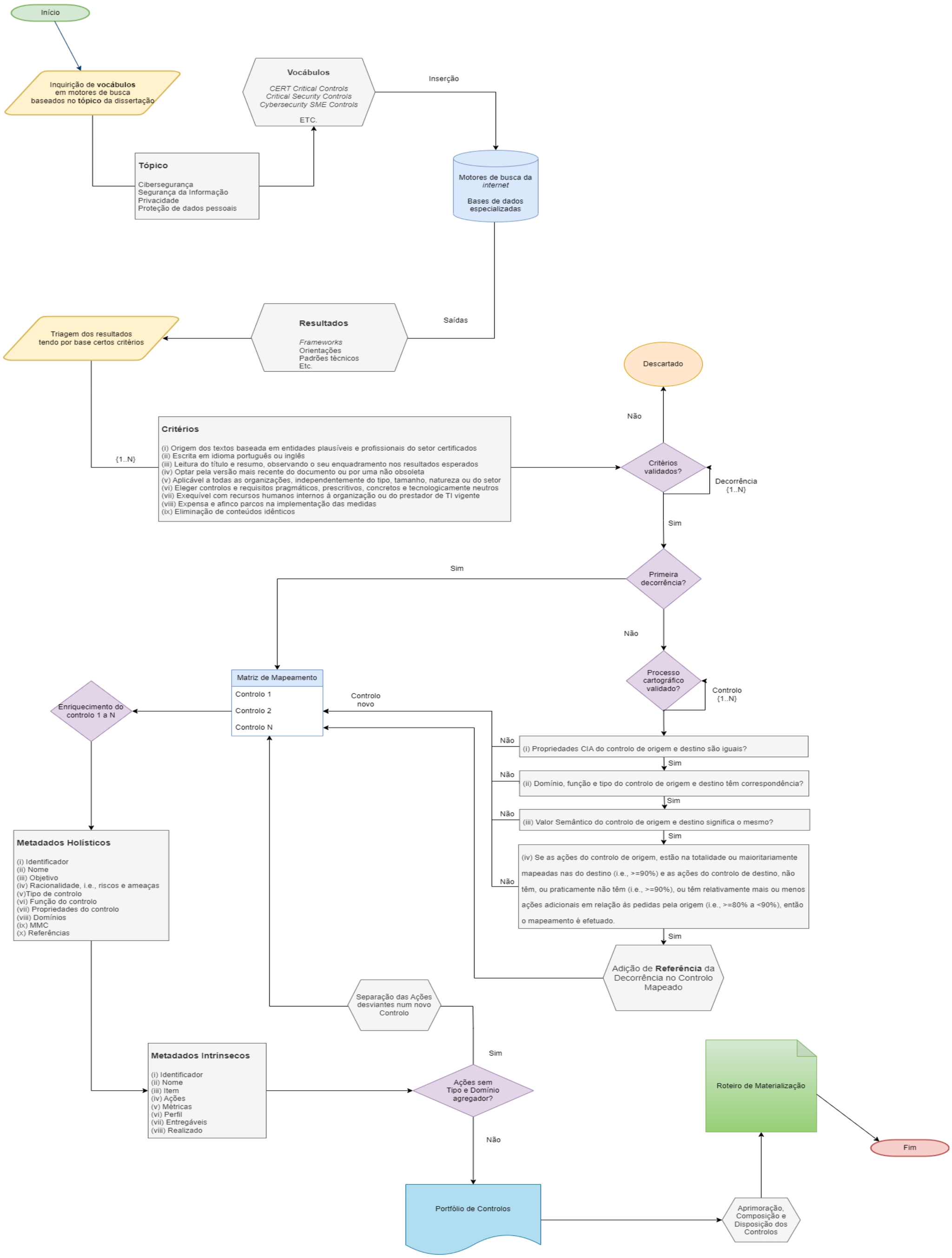


Figura 14: Metodologia Detalhe

4

DESENVOLVIMENTO

Neste capítulo apresenta-se a investigação, desconstrução e materialização de controlos normativos em ações práticas, basilares à proteção e persecução dos objetivos estratégicos das PME, no contexto corpóreo e espaço digital.

4.1 MATRIZ DE MAPEAMENTO

A Tabela 9 agrega a coleção de documentos observados e explorados minuciosamente, sustentada na metodologia apresentada no capítulo 3.

Tabela 9: Documentos de Suporte ao Portfólio de Controlos

#	Documento	RO	RE	Versão	Lançamento	ORG	O
GB.NCSC.CE	*Cyber Essentials: Requirements for IT Infrastructure*	5	7	3.0	Janeiro de 2022	NCSC	GB
NZ.CERT.NZ.CC	*CERT NZ's 2022 Critical Controls*	10	11	2022	Fevereiro de 2022	CERT NZ	NZ
US.NIST.SBIS.TF	*Small Business Information Security: The Fundamentals*	34	36	*Revision* 1	Novembro de 2016	NIST	US

Legenda: RO - Requisitos Originais | RE - Requisitos Extraídos | ORG - Organismo | O - Origem

O Apêndice C conglomera a completude dos controlos inferidos a partir dos suportes identificados na Tabela 9.

4.1.1 Cyber Essentials: Requirements for IT infrastructure

A seleção da *framework* introdutória, *Cyber Essentials: Requirements for IT infrastructure*, foi utilizada pelas seguintes razões principais: (i) proveniente de um organismo fidedigno; (ii) direcionado a SME; (iii) composto por parcos requisitos; (iv) necessário às empresas que queiram fazer negócio com o setor público na GB; (v) o custo de certificação variar entre as £300 e £500.

São introduzidos cinco temas técnicos de implementação obrigatória: (i) *firewalls*; (ii) *secure configuration*; (iii) *User access control*; (iv) *malware protection*; (v) *security update management*. Um tema técnico recomendado: *backup up your data*. Um tema organizacional obrigatório: *scope*. Uma leitura atenta e, tendo por base a Tabela 5, afigura-se a existência de ações em vários temas, que se encaixam mais harmoniosamente em diferentes famílias de controlos. Na Figura 15 visualizam-se no primeiro nível os requisitos originais da *framework*, no segundo patamar a derivação efetuada em termos de arrumação lógica dos controlos, mas mantendo-se imaculado o teor dos requisitos originais, e no terceiro degrau o número de ações obtidas em cada requisito, perfazendo 65.

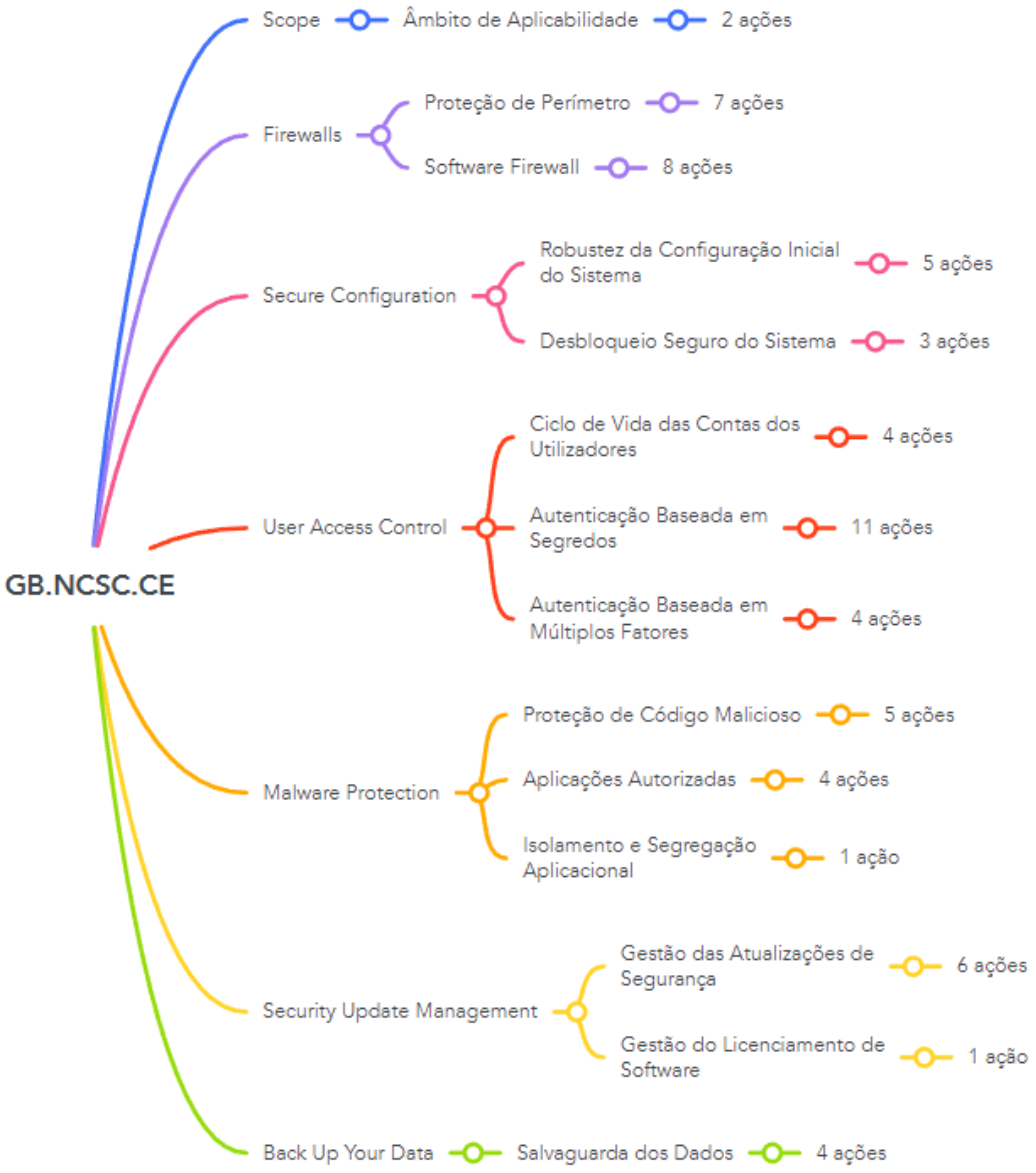


Figura 15: Desdobramento da *framework* GB.NCSC.CE

4.1.2 CERT NZ's Critical Controls 2022

A segunda *framework* escolhida, *CERT NZ's Critical Controls 2022*, desenvolve dez controlos baseados nos incidentes de cibersegurança vivenciados nos últimos 12 meses. A sua implementação correta, previne, deteta e contem a maioria dos ataques ocorridos no ano transato. Os controlos são desenhados para ajudar as pequenas e médias organizações a identificar onde devem investir os seus recursos financeiros e de tempo. Os mesmos são desenvolvidos tendo como suporte os dados e perceções, que o CERT da NZ recebeu, provenientes de relatórios e fontes de ameaças internacionais. Optou-se por bifurcar o controlo *Implementation multi-factor authentication and verification*, por existirem nitidamente ações de funcionalidade "técnica" e "administrativa" (Figura 16), mantendo-se, no entanto, a plenitude das 67 ações originais, descortinadas ao longo do documento.

Figura 16: Desdobramento da orientação NZ.CERT.NZ.CC

4.1.3 Small Business Information Security: The Fundamentals

A terceira escolha recai sobre a publicação, *Small Business Information Security: The Fundamentals*, onde se apresentam os fundamentos de um programa de segurança da informação, numa linguagem não técnica, para pequenos negócios. O controlo *Compreender as Ameaças e Vulnerabilidades do Negócio* é objeto de uma forqueamento pela predominância da tipologia "técnica" sobre as demais. No entanto, sem desvios ao texto original, conservando-se todas as ações num total de 143 (Figura 17).

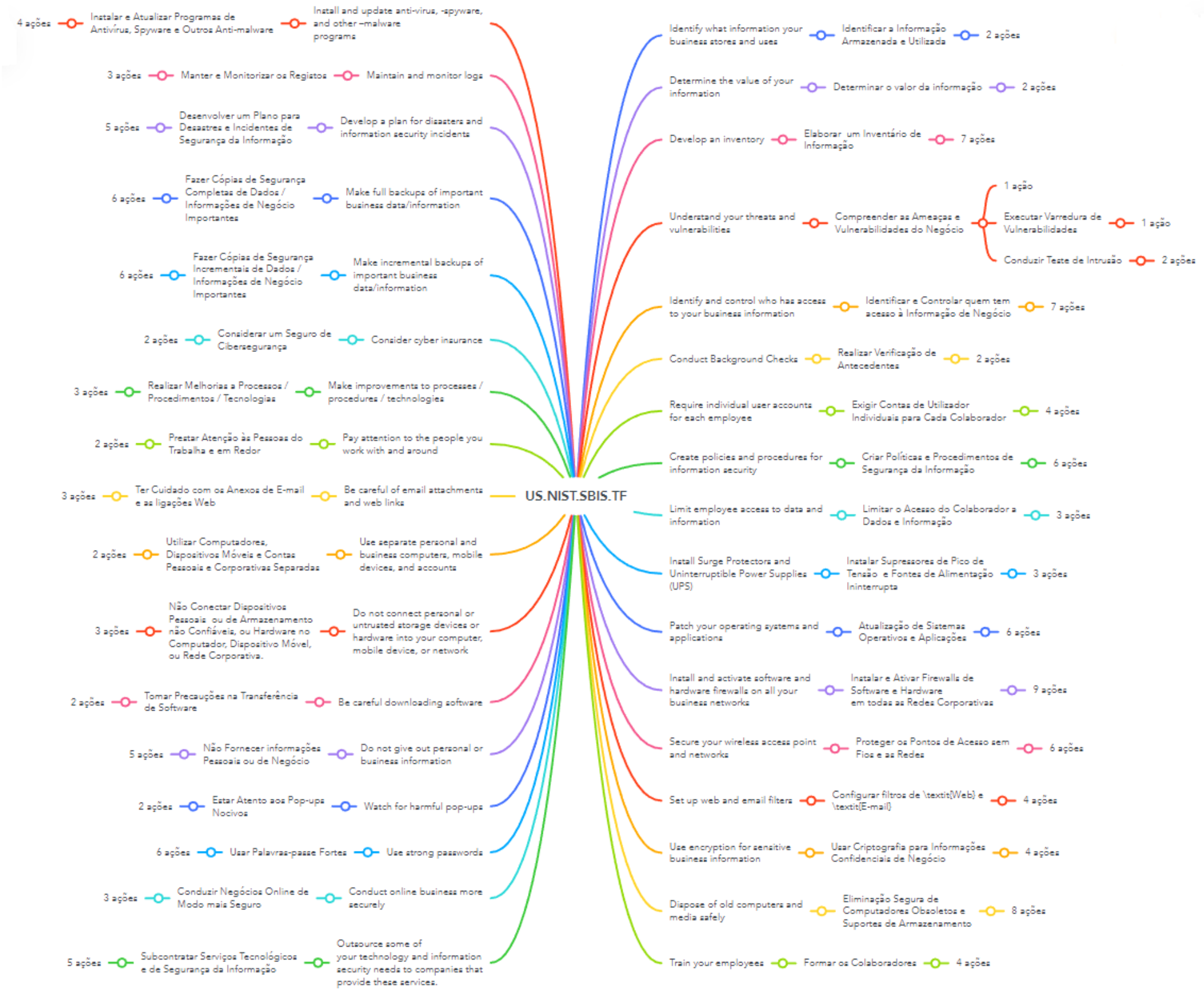


Figura 17: Desdobramento da publicação US.NIST.SBIS.TF

4.2 PORTFÓLIO DE CONTROLOS

O detalhe das ações dos controlos de cada *framework*, o perfil afeto e as métricas selecionadas, constituem o cerne a ser aclarado subsequentemente.

4.2.1 Cyber Essentials: Requirements for IT infrastructure

A Tabela 10 espelha os controlos da *framework* (NCSC, 2022). Dos 14 requisitos, três são do tipo Administrativo, 11 do tipo Técnico, 12 desempenham uma função Preventiva, enquanto nos campos Detetivo e Corretivo recai somente um; onze abarcam todas as propriedades CIA, dois focam-se na CI e existe um controlo tratando somente da A; sete Domínios são tidos em conta. Claramente estamos perante um guia focado nos aspetos mais técnicos e práticos da cibersegurança, direcionado para organizações que necessitam rapidamente de criar uma base de proteção sem complexidade excessiva.

Tabela 10: Portfólio de Controlos GB.NCSC.CE

Id	Nome	Objetivo	Racionalidade		T	F	Prop	Do	MMC	R
			Riscos	Ameaças						
1.7.1	Âmbito de Aplicabilidade	Determinar fronteiras e ativos aplicáveis sob a alçada dos controlos de segurança e privacidade da informação.	1,8,22 (...)	11,35,46 (...)	Adm	P	CIA	7	Caótico	Ref
1.14.2	Proteção de Perímetro	Assegurar que apenas serviços de rede seguros e necessários são acedidos a partir da *internet*.	10,18,19 (...)	1,3,29 (...)	Tec	P	CIA	14	Caótico	Ref
1.14.3	*Software Firewall*	Utilizar em dispositivos (e.g., portáteis) quando usados em redes não seguras (e.g., acessos *wi-fi* públicos).	10,18,19 (...)	1,3,29 (...)	Tec	P	CIA	14	Caótico	Ref
1.6.4	Robustez da Configuração Inicial do Sistema	Minimizar potenciais vulnerabilidades e aumentar a proteção contra-ataques informáticos comuns.	13,18,21 (...)	10,14,32 (...)	Tec	P	CI	6	Caótico	Ref
1.6.5	Desbloqueio Seguro do Sistema	Assegurar mecanismos de desbloqueio (e.g., PIN no telemóvel, biometria ou credencial no portátil) apropriados, aquando da necessidade da interação física do utilizador, para ganhar acesso aos serviços oferecidos pelo dispositivo.	10,12,18 (...)	1	Tec	P	CI	6	Caótico	Ref
1.9.6	Ciclo de Vida das Contas dos Utilizadores	Processo de aprovisionamento e remoção das contas dos utilizadores.	15	11,13,14 (...)	Adm	P	CIA	9	Caótico	Ref
1.9.7	Autenticação Baseada em Segredos	Autenticar os utilizadores antes de se conceder acesso a aplicações ou dispositivos.	10,13,18 (...)	28,41,45 (...)	Tec	P	CIA	9	Caótico	Ref
1.9.8	Autenticação Baseada em Múltiplos Fatores	Proteção extra na autenticação dos utilizadores antes de se conceder acesso a aplicações ou dispositivos.	10,18,21 (...)	12,37,41 (...)	Tec	P	CIA	9	Caótico	Ref
1.10.9	Proteção de Código Malicioso	Detetar e desabilitar programas maliciosos antes de provocarem danos a sistemas.	5,8,12 (...)	26,30,32 (...)	Tec	P	CIA	10	Caótico	Ref
1.6.10	Aplicações Autorizadas	Executar somente programas confiáveis e aprovados.	4,10,13 (...)	10,26,30 (...)	Tec	P	CIA	6	Caótico	Ref
1.14.11	Isolamento e Segregação Aplicacional	Isolamento de componentes não confiáveis durante a execução num ambiente controlado (*sandboxing*).	13,18,19 (...)	15,27,29 (...)	Tec	P	CIA	14	Caótico	Ref
1.11.12	Gestão das Atualizações de Segurança	Assegurar que programas e dispositivos não se encontram vulneráveis a falhas de segurança conhecidas.	18	47	Tec	P	CIA	11	Caótico	Ref
1.6.13	Gestão do Licenciamento de *Software*	*Software* é usado consoante os contratos acordados e legislação em vigor.	4,5,6 (...)	46	Adm	D	CIA	6	Caótico	Ref
1.13.14	Salvaguarda dos Dados	Criar cópia(s) da informação e salvaguardá-la num outro dispositivo ou na nuvem.	5,13	30	Tec	C	A	13	Caótico	Ref

Id - Identificador | T - Tipo [Adm - Administrativo, Tec - Técnico] | F - Função [P - Preventivo, D - Detetivo, C - Corretivo,] | Prop - Propriedades |Do - Domínios | Ref - GB.NCSC.CE

Das Tabelas 11 à 24 consubstanciam-se as ações imprescindíveis à efetivação da presente *framework*. Embora, à primeira vista, possa parecer de fácil implementação, dez ações foram desviadas do perfil Nuclear para o Definido (oito) e Otimizado (duas), tendo em conta a insapiência das PME nacionais, conforme narrado nas tabelas sequentes.

Para cada controlo há um número ilimitado de métricas possíveis de se estipular. As métricas selecionadas permitem aferir a eficácia e eficiência de cada controlo e por isso são as eleitas, perfazendo 35.

Os entregáveis alcançados, materializam as evidências substanciais de cada controlo.

Nas opções das ações, existem seis que se enquadram na etiqueta “Recomendado”, quatro na “Alternativa” e cinco na de “Complemento”.

Tabela 11: Âmbito de Aplicabilidade

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.7.1	Âmbito de Aplicabilidade	1	Estababelecimento dos limites do âmbito.	-	1. Qual é a % dos ativos (e.g., departamentos, pessoas, localizações)	Nc	D	N
		2	Determinar os ativos no limite definido.	-	da organização incluídos dentro do âmbito de aplicabilidade?	Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 12: Proteção de Perímetro

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.14.2	Proteção de Perímetro	1	Modificar as senhas administrativas por defeito para alternativas mais robustas.	Com	1. Número de tentativas de intrusão na rede?	Nc	E	N
		2	Desabilitar o acesso remoto administrativo.		2. Número de pacotes falso positivos descartados, devido a regras criadas?	Nc		N
		3	Prevenir o acesso à *interface* de administração, usada na gestão de configuração da *firewall*, a partir da *internet*.	Alt	3. % de memória, CPU, disco, largura de banda, etc. utilizada? 4. Taxa de pacotes de entrada e saída que são aceites, rejeitados, descartados, e registados por interface da *firewall*?	Nc		N
		4	Em caso de necessidade de acesso à consola de gestão a partir da *internet*, documentar o caso de uso e proteger a *interface*, através de autenticação multifator ou usando uma lista restrita de endereços IP, em adição a um mecanismo de gestão de senhas fiável.		5. Taxa de sessões (e.g., FTP, HTTP, SMTP) que resultam em falhas de autorização? 6. Número de vezes que uma regra de aplicação é ativada?	Df		N
		5	Bloquear ligações de entrada não autenticadas por defeito.	-		Nc		N
		6	Assegurar e documentar a aprovação das regras de entrada da *firewall*, incluindo o caso de uso, por um indivíduo autorizado.	-		Df		N
		7	Remover ou desabilitar regras de *firewall* não necessárias de modo expedito.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 13: *Software Firewall*

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.14.3	*Software Firewall*	1	Modificar as senhas administrativas por defeito para alternativas mais robustas.	Com	1. Número de tentativas de intrusão no dispositivo? 2. Número de pacotes falso positivos descartados, devido a regras criadas? 3. Taxa de pacotes de entrada e saída que são aceites, rejeitados, descartados, e registados por interface da *firewall*?	Nc	E	N
		2	Desabilitar o acesso remoto administrativo.			Nc		N
		3	Prevenir o acesso à *interface* de administração, usada na gestão de configuração da *firewall*, a partir da *internet*.	Alt		Nc		N
		4	Em caso de necessidade de acesso à consola de gestão a partir da *internet*, documentar o caso de uso e proteger a *interface*, através de autenticação multifator ou usando uma lista restrita de endereços IP, em adição a um mecanismo de gestão de senhas fiável.			Df		N
		5	Bloquear ligações de entrada não autenticadas por defeito.	-		Nc		N
		6	Assegurar e documentar a aprovação das regras de entrada da *firewall*, incluindo o caso de uso, por um indivíduo autorizado.	-		Df		N
		7	Remover ou desabilitar regras de *firewall* não necessárias de modo expedito.	-		Nc		N
		8	Utilizar a *firewall* pré-instalada do sistema operativo em detrimento de aplicações de terceiras partes.	Rec		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 14: Robustez da Configuração Inicial do Sistema

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.6.4	Robustez da Configuração Inicial do Sistema	1	Remover e desabilitar contas de utilizador não necessárias (e.g., contas convidados, contas de administração).	-	1. Número de listas de verificação e guiões (*scripts*) aplicados, de modo a fortalecer a configuração dos sistemas?	Nc	F	N
		2	Modificar senhas de contas por defeito ou fáceis de adivinhar.	-		Nc		N
		3	Remover ou desabilitar *software* não necessário (e.g., aplicações, utilitários de sistema, serviços de rede).	-		Nc		N
		4	Desabilitar qualquer capacidade de autoexecução, que permita a execução de ficheiros sem autorização do utilizador, como, por exemplo, quando são descarregados a partir da *internet*.	-		Nc		N
		5	Garantir autenticação dos utilizadores antes de se permitir o acesso a serviços ou dados organizacionais.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 15: Desbloqueio Seguro do Sistema

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.6.5	Desbloqueio Seguro do Sistema	1	Bloquear o dispositivo após, no máximo, 10 tentativas falhadas de autenticação.	Com	1. Número de contas bloqueadas num determinado intervalo de tempo? 2. Lista e origem de IP das contas bloqueadas?	Nc	G	N
		2	Estrangular (*throttling*) o ritmo das tentativas de acesso. O Tempo de espera entre cada tentativa falhada aumenta. Não se deve permitir mais de 10 tentativas num espaço temporal de 5 minutos.			Nc		N
		3	O segredo usado somente no ato de desbloqueio deve ter pelo menos 6 caracteres.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 16: Ciclo de Vida das Contas dos Utilizadores

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.9.6	Ciclo de Vida das Contas dos Utilizadores	1	Processo de criação e aprovação da conta do utilizador.	-	1. Taxa de utilizadores removidos face aos dados provenientes dos RH?	Nc	H	N
		2	Desabilitar ou remover a conta de utilizador quando não é mais requerida (e.g., utilizador saiu da organização, conta não é utilizado durante um certo período temporal).	-	2. Número de utilizadores com revisão de privilégios, após mudança de funções em relação ao total de mudanças?	Nc		N
		3	Usar conta separada no desempenho de atividades privilegiadas.	-	3. Quantidade de utilizadores com acesso de administração de sistema, que possuem igualmente uma conta de utilizador normal?	Nc		N
		4	Remover ou desabilitar privilégios de acesso especiais, quando não são mais necessários (e.g., após alteração de funções).	-	4. A contagem das contas criadas de utilizadores iguala o número de pedidos recebidos dos RH?	Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 17: Autenticação Baseada em Segredos

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.9.7	Autenticação Baseada em Segredos	1	Todas as contas de utilizadores obrigam à utilização de um mecanismo de autenticação.	-	1. % de utilizadores sem um gestor de senhas? 2. Número de senhas fracas e comuns em utilização?	Nc	I	N
		2	Atribuir credencias únicas a cada utilizador.	-		Nc		N
		3	Bloquear o dispositivo após, no máximo, 10 tentativas falhadas de autenticação.	Com		Nc		N
		4	Estrangular (*throttling*) o ritmo das tentativas de acesso. O Tempo de espera entre cada tentativa falhada aumenta. Não se deve permitir mais de 10 tentativas num espaço temporal de 5 minutos.			Nc		N
		5	Cada senha deve ter no mínimo 12 caracteres, sem restrições em relação ao tamanho máximo.	Com		Nc		N
		6	Cada senha deve ter no mínimo 8 caracteres, sem restrições em relação ao tamanho máximo, e uso automático de bloqueio de palavras-chave, aplicando uma lista de negação.			Nc		N
		7	Educar os utilizadores a evitar escolher senhas fracas e comuns, e optar por segredos de tamanho longo.	-		Nc		N
		8	Utilizar um gestor de senhas.	-		Nc		N
		9	N obrigar à expiração das palavras-passe.	-		Nc		N
		10	N forçar requisitos de complexidade dos segredos.	-		Nc		N
		11	Existir um processo de troca da palavra-passe, se o utilizador suspeitar ou souber de comprometimento da mesma.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 18: Autenticação Baseada em Múltiplos Fatores

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.9.8	Autenticação Baseada em Múltiplos Fatores	1	Contas de administração dos dispositivos devem usar mais do que um fator.	-	1. % de contas privilegiadas sem um segundo fator de autenticação?	Df		N
		2	Contas acessíveis a partir da *internet* (e.g., autenticação em serviços na nuvem) devem sempre usar mais do que um fator.	-	2. % de contas privilegiadas onde o segundo fator de autenticação é o SMS?	Nc	I	N
		3	Cada senha deve ter no mínimo 8 caracteres, sem restrições em relação ao tamanho máximo.	-	3. Número de contas de utilizadores regulares com acesso a serviços na nuvem sem um segundo fator de autenticação ativado?	Nc		N
		4	Utilização de SMS como segundo fator, somente se não existir alternativas, como, aplicação num telemóvel corporativo ou *token* físco.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 19: Proteção de Código Malicioso

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.10.9	Proteção de Código Malicioso	1	Atualização das assinaturas de código malicioso pelo menos diariamente.	-	1. % de máquinas sem o motor de assinatura atualizado?	Nc		N
		2	Acesso aos ficheiros alvo de varredura automática, incluindo quando os ficheiros são descarregados e abertos, e quando são acedidos a partir de uma partilha de rede.	-	2. Número de vírus detetados e não limpos? 3. Quantidade de máquinas com alertas não verificados?	Nc	K	N
		3	Acesso a páginas *web*, por um navegador, são objeto de varredura automática.	-	4. Top 50 dos sítios *web* visitadas não contem conteúdos considerados inapropriados conforme as políticas da organização?	Nc		N
		4	O *software* previne ligações a páginas maliciosas na *internet* (e.g., por uma lista de negação).	Alt		Nc		N
		5	Caso de uso documentado pelo não bloqueio a páginas maliciosas na *internet* e o utilizador compreende e aceita o risco associado.			Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 20: Aplicações Autorizadas

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.6.10	Aplicações Autorizadas	1	Somente aplicações aprovadas podem ser instaladas e executadas nos dispositivos.	-	1. Taxa de aplicações não controladas (*Shadow* IT)? 2. Número de aplicações instaladas, não assinadas digitalmente?	Nc		N
		2	Somente aplicações assinadas digitalmente (*code signing*) podem ser instaladas e executadas nos dispositivos.	-		Ot	L	N
		3	Manter uma lista de aplicações aprovadas.	-		Nc		N
		4	Utilizadores não podem conseguir instalar aplicações não assinadas ou com assinatura inválida.	-		Df		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 21: Isolamento e Segregação Aplicacional

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.14.11	Isolamento e Segregação Aplicacional	1	Todo o código, de origem desconhecida, tem de ser executado num ambiente controlado (*sandbox*), que previna acesso a outros recursos, exceto caso haja permissão explícita do utilizador.	-	1. % de código desconhecido executado em ambiente controlado?	Df	L	N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 22: Gestão das Atualizações de Segurança

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.11.12	Gestão das Atualizações de Segurança	1	Todo o *software* tem a atualização automática habilitada, sempre que possível.	-	1. % de programas em uso sem suporte por parte do fabricante? 2. Taxa de programas atualizados consoante a janela temporal definida?	Nc	M	N
		2	Só são usados programas suportados pelos fabricantes.	-		Nc		N
		3	Removido dos dispositivos sempre que o período de suporte tenha caducado (EOL).	Alt		Nc		N
		4	Isolado num ambiente separado através de uma *firewall* ou VLAN, bloqueando-se todo o tráfego de e para a *internet*.			Df		N
		5	Aplicar todos os remendos de segurança (*security patches*), incluindo, todas as configurações manuais necessárias, no prazo de 14 dias, quando: (i) a atualização é etiquetada pelo fabricante como "crítica" ou de "risco elevado"; (ii) a atualização endereça vulnerabilidades com um resultado CVSS de 7 ou superior; (iii) não há indicação do nível da vulnerabilidade que a atualização fornecida pelo fabricante resolve.	-		Nc		N
		6	Todos os remendos de segurança são aplicados no prazo máximo de 14 dias.	Rec		Ot		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 23: Gestão do Licenciamento de *Software*

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.6.13	Gestão do Licenciamento de *Software*	1	Todo o *software* em utilização encontra-se licenciado.	-	1. % de *software* licenciado?	Nc	N	N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 24: Salvaguarda dos Dados

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.13.14	Salvaguarda dos Dados	1	Salvaguardar a informação regularmente.	Rec	1. Número de salvaguardas terminadas com avisos ou erros? 2. Taxa de salvaguardas críticas copiadas para outra localização? 3. Número de salvaguardas repostas para efeitos de teste?	Nc	O	N
		2	Copiar a informação salvaguardada num outro repositório local ou remoto.	Rec		Nc		N
		3	Habilitar salvaguardas automáticas, sempre que possível.	Rec		Nc		N
		4	Salvaguardas efetuadas para discos externos USB devem ser desconectados após a realização da tarefa.	Rec		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

4.2.2 CERT NZ's Critical Controls 2022

A Tabela 25 descreve os controlos da *framework* (NZ, 2022), num somatório de 11 exigências, três das quais do tipo Administrativo, oito do tipo Técnico, nove funcionam num papel Preventivo e uma, no campo Detetivo e outra no Corretivo. Oito famílias de controlos estão representadas. Nota-se uma tendência de valorização dos aspetos técnicos operacionais, em detrimento de processos, o que é natural, visto tratar-se de um guia de combate pragmático ao cibercrime e não direcionado às políticas.

Tabela 25: Portfólio de Controlos NZ.CERT.NZ.CC

Id	Nome	Objetivo	Racionalidade		T	F	Prop	Do	MMC	R
			Riscos	Ameaças						
1.11.15	Atualização do *Software* e Sistemas	Manter todo o *software* (dos sistemas operativos e aplicações às *firewalls* e *routers*) atualizado.	18	47	Tec	P	CIA	11	Caótico	Ref
1.9.16	Implementar Autenticação Múltiplos Fatores e Verificação	Prevenir acessos não autorizados sobretudo a contas privilegiadas e acessíveis a partir da *internet*.	10,18,21 (...)	12,37,41 (...)	Tec	P	CIA	9	Caótico	Ref
1.9.17	Providenciar e Utilizar um Gestor de Segredos	Aumentar a possibilidade dos utilizadores usarem senhas fortes e diferentes em cada sistema, e facilitar a partilha de palavras-chave de acesso a contas multiutilizador.	18	10	Tec	P	C	9	Caótico	Ref
1.2.18	Configuração de Registos e Alertas	Receber registos (*logs*) de todos os ativos e identificar eventos-chave, são atividades cruciais na deteção e investigação de incidentes.	4, 10, 15 (...)	3,4,10 (...)	Tec	D	CIA	2	Caótico	Ref
1.6.19	Ciclo de Vida dos Ativos	Rastrear o *sofwtare* e *hardware* em cada fase chave, i.e., aquisição ou desenvolvimento, manutenção e desativação.	5,18, 21 (...)	1, 30, 35 (...)	Adm	P	CIA	6	Caótico	Ref
1.13.20	Implementar e Testar as Salvaguardas	Recuperar rápido e eficazmente após uma disrupção causada por um incidente ou ciberataque.	5,13	30	Tec	C	A	13	Caótico	Ref
1.10.21	Implementar Controlo Aplicacional	Prevenir ficheiros maliciosos, como o *malware*, de executarem no sistema.	5,8,12 (...)	26,30,32 (...)	Tec	P	CIA	10	Caótico	Ref
1.5.22	Aplicar o Princípio do Menor Privilégio	Precaver os utilizadores de acidentalmente ou intencionalmente realizarem alterações, que possam causar incidentes de segurança.	6,15,16 (...)	1,7,13 (...)	Adm	P	CIA	5	Caótico	Ref
1.14.23	Implementar Segmentação de Rede	Sem uma segmentação de rede efetiva, atores maliciosos podem-se movimentar livremente pela rede e ganhar acesso a sistemas adicionais.	18,19,21 (...)	1,14,23 (...)	Tec	P	CIA	14	Caótico	Ref
1.6.24	Definir Padrões Seguros para Macros	Atacantes usam macros para camuflar programas maliciosos. O uso de configurações restritas pode prevenir a execução e propagação desses *malwares*.	10,18,21 (...)	10,14,32 (...)	Tec	P	CI	6	Caótico	Ref
1.9.25	Implementar Processo de Negócio de Verificação	Certificar da existência de processos em vigor para verificar alterações sensíveis, tais como, reinicialização de palavras-passe ou alterações onde haja transações financeiras significativas.	5,8,12 (...)	22,32,37 (...)	Adm	P	CI	9	Caótico	Ref

Id - Identificador | T - Tipo [Adm - Administrativo, Tec - Técnico] | F - Função [P - Preventivo, D - Detetivo, C - Corretivo,] | Prop - Propriedades |Do - Domínios | Ref - NZ.CERT.NZ.CC

A partir da Tabela 26 à 36 estão designadas as ações com vista ao cumprimento dos princípios supraditos. Destaque-se a existência de 16 regras catalogadas no perfil Definido, somente uma no Otimizado, e 29 métricas, que auxiliam na compreensão do sucesso de implementação das ações propostas.

Tabela 26: Atualização do *Software* e Sistemas

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.11.15	Atualização do *Software* e Sistemas	1	Dispor de uma visão completa do *software* no ambiente TI. Todos os dias, é possível se saber que novo *software* é adicionado e quais são os atuais níveis de *patch*.	-	1. Taxa de *software* controlado pelo departamento de TI? 2. Número de pacotes de *software* atualizados manualmente? 3. % de atualizações canceladas e diferidas?	Nc	M	N
		2	Atualizar todos os sistemas com as últimas correções.	-		Nc		N
		3	Possuir uma estratégia abrangente de gestão de correções, que abranja todo o *software* dos sistemas: identificação, prioritização, agendamento, testes, e manuseamento.	-		Nc		N
		4	Existir um processo de correção, na sua maioria automatizado, que incluía a automatização da notificação, identificação, transferência, verificação, *packaging*, salvaguarda, testes, e implementação de correções. As ações que requerem a avaliação do risco ou a realização de avaliações, continuam a ser manuais.	-		Nc		N
		5	Reavaliar a cada ciclo de correção, o risco de se realizar ou não a correção, dos remendos cancelados ou diferidos.	-		Nc		N
		6	Existir documentação de apoio e informação à disposição dos utilizadores da organização, para os informar sobre a estratégia e a importância da aplicação de correções.	-		Nc		N
		7	Compreender o risco associado aos atuais níveis de remendo do ambiente TI da organização e trabalhar para mitigar o risco.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 27: Implementar Autenticação Múltiplos Fatores

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.9.16	Implementar Autenticação Múltiplos Fatores	1	Todos os serviços administrativos, sistemas voltados para a *internet* e outros sistemas críticos para a organização, exigem aos utilizadores a utilização de MFA no acesso. Sem MFA habilitado, o acesso é impossibilitado.	-	1. % de utilizadores com MFA habilitado? 2. % de sistemas críticos, sistemas com *interfaces* expostas à *internet* e sistemas de processamento administrativo, que exigem a utilização de autenticação de dois ou mais fatores? 3. Número de eventos suspeitos registados, diretamente relacionados com autenticação nos últimos trê meses?	Ot	I	N
		2	Os métodos de MFA utilizados não têm vulnerabilidades conhecidas e não são depreciados por organismos de configuração padrão (e.g., NIST).	-		Df		N
		3	Para os sistemas geridos e detidos pela organização, o módulo de autenticação MFA é mantido atualizado. Quaisquer dependências relacionadas do módulo são também mantidas atualizadas. A infraestrutura onde o módulo funciona é robustecida, i.e., atualizada e as portas não utilizadas são bloqueadas.	-		Nc		N
		4	Alterações de configurações e políticas relativas ao MFA e tentativas de autenticação suspeitas, negadas ou de contorno, são registadas e armazenadas num local de registos central.	-		Df		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 28: Providenciar e Utilizar um Gestor de Segredos

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.9.17	Providenciar e Utilizar um Gestor de Segredos	1	Existir um programa de gestão de segredos aprovado para uso na organização e fornecido a todos os utilizadores.	-	1. Taxa de utilizadores com formação na operação do gestor de palavras-passe? 2. % de senhas em utilização expostas em base de dados na *internet*?	Nc	P	N
		2	Consciencializar todos os utilizadores para a importância e obrigatorieda do seu uso.	-		Nc		N
		3	Controlo de acessos e gestão de políticas centralizadas.	-		Df		N
		4	Definir uma política de criação de segredos longos e únicos.	-		Df		N
		5	Suportar e fornecer documentação que permita aos utilizadores o manuseamento eficiente da ferramenta.	-		Nc		N
		6	Ativar o *logging* para segredos partilhados.	-		Df		N
		7	Impor a obrigatoriedade de MFA no acesso à ferramenta.	-		Df		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 29: Configuração de Registos e Alertas

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.2.18	Configuração de Registos e Alertas	1	Habilitar o registo para eventos críticos para o negócio ou que envolvem dados sensíveis.	-	1. % de ativos com registo de eventos configurados? 2. % de ativos importantes para o negócio com registo de eventos configurados? 3. Número de alertas com resposta automatizada? 4. Taxa de fontes de eventos, que enviam os registos para um sistema centralizado?	Nc	Q	N
		2	Sincronizar todos os sistemas à mesma fonte temporal e a um fuso horário consistente, para facilitar a análise e correlação.	-		Nc		N
		3	Enviar os registos para um sistema de armazenamento e análise centralizado.	-		Df		N
		4	O sistema central de agregação de registos deve ter um acesso limitado, somente de leitura, aos utilizadores que dele necessitam. Alterações e eliminação de registos não deve ser possível.	-		Nc		N
		5	Anotar quaisquer modificações à configuração do sistema de registo central.	-		Nc		N
		6	Criar alertas e relatórios automáticos, para eventos suspeitos ou invulgares.	-		Df		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 30: Ciclo de Vida dos Ativos

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.6.19	Ciclo de Vida dos Ativos	1	Registar todos os ativos de sistema, incluindo *software* e *hardware*.	-	1. Taxa de registo de novos ativos nos últimos três meses? 2. % de ativos configurados com parametrizações de segurança antes de serem utilizados no ambiente de produção? 3. Número de ativos em uso sem suporte do fabricante? 4. Número de ativos em uso após fim do ciclo de vida?	Nc	R	N
		2	Registar todos os novos ativos aquando da sua aquisição ou desenvolvimento.	-		Nc		N
		3	Todos os ativos são objeto de parametrizações de robustez antes de serem utilizados, sendo mantidos regularmente com atualizações e correções.	-		Nc		N
		4	Ativos que se aproximam do fim de vida ou do fim de suporte por parte do fornecedor, têm um plano de desmantelamento antes de se tornarem sistemas obsoletos.	-		Df		N
		5	Os ativos desativados são removidos do meio envolvente e destruídos em segurança.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 31: Implementar e Testar as Salvaguardas

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.13.20	Implementar e Testar as Salvaguardas	1	O responsável por cada conjunto de dados toma decisões em torno da importância e dos tempos de recuperação dos mesmos (objetivos de recuperação). A equipa de TI fornece aconselhamento sobre os objetivos de recuperação.	-	1. % de conjuntos de dados classificados com tempos de recuperação determinados? 2. % de conjunto de dados com testes de recuperação completos nos prazos acordados?	Nc	O	N
		2	As cópias de segurança são realizadas automática e regularmente. O calendário é baseado nos objetivos de recuperação da organização.	-		Nc		N
		3	Enviar alertas para quaisquer falhas de cópias à equipa responsável pelas salvaguardas e aos donos dos dados.	-		Nc		N
		4	Testar regularmente as cópias de segurança usando diferentes casos de uso. Por exemplo, testar a reposição de um único ficheiro, pelo menos uma vez por trimestre, e testar uma recuperação completa, pelo menos uma vez por ano.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 32: Implementar Controlo Aplicacional

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.10.21	Implementar Controlo Aplicacional	1	A organização tem *software* instalado em todos os dispositivos, que fazem cumprir as políticas de controlo de aplicações.	-	1. % de dispositivos com *software* de deteção e resposta de *endpoint* instalado? 2. Número de políticas de controlo aplicacional ativadas?	Nc	L	N
		2	As políticas de controlo de aplicações, são automaticamente geridas, utilizando algoritmos de aprendizagem de comportamento, entre outros. Políticas e regras também podem ser criadas e aplicadas manualmente pelos administradores de sistemas.	-		Nc		N
		3	A organização impõe controlos de acesso, que permitem a aplicação das políticas certas aos utilizadores corretos.	-		Nc		N
		4	Aplicar o princípio do menor privilégio, limitando a capacidade de os utilizadores contornarem as políticas de controlo de aplicações estabelecidas.	-		Nc		N
		5	Monitorizar as técnicas conhecidas de contorno de políticas, e incluir este conhecimento, no processo de gestão de vulnerabilidades.	-		Df		N
		6	O processo de robustez da configuração inicial dos sistemas, inclui a instalação de *software* de segurança em quaisquer novos dispositivos, i.e., estações de trabalho, servidores, computadores portáteis, dispositivos móveis, e qualquer outro dispositivo, que aceda a dados organizacionais. Isto pode incluir dispositivos de propriedade da organização e BYOD.	-		Nc		N
		7	Os eventos das políticas de controlo de aplicações, são registados e armazenados num local central, para capturar tentativas e negações de execução de ficheiros. Os registos são configurados para desencadear alertas, que alimentam processos operacionais, tais como, a gestão de incidentes ou de alterações. Um processo de gestão de alterações de emergência é seguido, quando programas críticos são bloqueados.	-		Df		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 33: Aplicar o Princípio do Menor Privilégio

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.5.22	Aplicar o Princípio do Menor Privilégio	1	Perceber o nível mínimo de permissões necessárias, para todos os utilizadores na organização.	-	1. Número de vezes em que há revisão das permissões de todas as contas privilegiadas por ano? 2. % de funções com nível de permissões pré-definidas, englobando todas as aplicações e sistemas de que necessitam? 3. Quantidade de regras criadas mapeando a ocorrência de cenários de uso anómalos?	Nc	S	N
		2	Compreender as permissões atribuídas a funções dentro de cada sistema. Isto permite saber, se um utilizador com essa função, tem as permissões certas para o seu trabalho.	-		Nc		N
		3	Visão completa das permissões e funções que cada utilizador tem para cada sistema.	-		Nc		N
		4	Conhecer a totalidade dos sistemas na organização e como os utilizadores os acedem, quer através da *interface* frontal de uma aplicação, quer através da infraestrutura de suporte. Isto inclui contas de utilizador em uso, e contas de sistema e serviços, que não são acedidas regularmente pelos utilizadores.	-		Nc		N
		5	Identificar as permissões de que um utilizador necessita antes de atribuir ou alterar qualquer acesso.	-		Nc		N
		6	Rever os acessos dos utilizadores para garantir, que mantêm o menor nível de permissões necessárias para o seu trabalho.	-		Nc		N
		7	Identificar a ocorrência de mudanças, que podem obrigar a realização de alterações nas permissões, funções ou utilizadores de um sistema.	-		Nc		N
		8	Remover utilizadores que já não são necessários.	-		Nc		N
		9	Atribuir contas separadas a utilizadores que necessitem de permissões administrativas ou sensíveis. Uma conta tem as permissões administrativas, e a outra tem permissões menores para outros aspetos do seu trabalho.	-		Nc		N
		10	Registar as ações tomadas pelos utilizadores administrativos e enviar os eventos para um repositório central para análise e alerta. Configurar regras de envio de notificações, quando ações inesperadas acontecem, tais como, alterações durante horas invulgares do dia.	-		Df		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 34: Implementar Segmentação de Rede

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.14.23	Implementar Segmentação de Rede	1	Todos os dispositivos sensíveis, estão separados de outros sistemas sendo mantidos em redes segmentadas.	-	1. Número de redes existentes na organização? 2. % de dispositivos de rede configurados com regras de negação de todo o tráfego por defeito?	Nc	T	N
		2	Todas as redes críticas, são isoladas de redes não fidedignas ou de baixa confiança.	-		Nc		N
		3	Todos os dispositivos de rede negam tráfego por defeito.	-		Nc		N
		4	Todas as redes têm regras para permitir apenas portas e protocolos, necessários para os dispositivos dessa rede funcionarem.	-		Nc		N
		5	Todos os dispositivos da rede são robustecidos e mantidos.	-		Nc		N
		6	Todo o acesso dos utilizadores à rede da organização requer autenticação.	-		Df		N
		7	Os eventos são registados e armazenados num local central, para capturar alterações de segurança e de configuração de autenticação nos dispositivos de rede e nas suas regras, tráfego de rede suspeito e tentativas de autenticação.	-		Df		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 35: Definir Padrões Seguros para Macros

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.6.24	Definir Padrões Seguros para Macros	1	Todos os utilizadores têm as macros desativadas por defeito e não as podem reativar.	-	1. Número de utilizadores inserido no grupo das macros?	Nc	K	N
		2	As macros são ativadas numa base de grupo de utilizadores. Apenas os utilizadores com necessidade de aceder a macros são adicionados ao grupo.	-		Nc		N
		3	A configuração do grupo de utilizadores só permite a execução de macros a partir de uma localização confiável.	Conplemento		Nc		N
		4	A configuração do grupo de utilizadores só permite a execução de macros assinadas digitalmente.			Df		N
		5	O grupo de utilizadores com macros é revisto, para assegurar, que todos os utilizadores ainda necessitam dessa funcionalidade (e segue o princípio do menor privilégio).	-		Nc		N
		6	Os registos são anotados e armazenados num local central, para capturar a execução de tipos de ficheiros com macros, tais como, .DOCM, .PPTM, .XLSM.	-		Df		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 36: Implementar Processo de Negócio de Verificação

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.9.25	Implementar Processo de Negócio de Verificação	1	Saber que equipas ou utilizadores na organização recebem pedidos externos, ou têm acesso a dados, para realizar pagamentos ou fazer alterações.	-	1. Número de tentativas de burlas ou fraudes financeiras detetadas no último ano fiscal? 2. % de alterações provenientes de origens externas (e.g., reinicialização de palavra-passe de prestador de serviço) ou pagamentos avultados verificadas nos últimos três meses? 3. Número de utilizadores com autorização à realização de pagamentos ou execução de pedidos externos?	Nc	U	N
		2	Elaborar um processo, seguido pelos utilizadores, para verificar todos os pedidos num canal de comunicação separado, antes de serem executados.	-		Nc		N
		3	Relatar e registar todos os eventos de segurança e pedidos não autorizados como parte do processo de gestão de incidentes de segurança da sua organização.	-		Nc		N
		4	Comunicar tentativas de burlas ou fraudes aos outros utilizadores, para poderem estar atentos a atividades semelhantes.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

4.2.3 Small Business Information Security: The Fundamentals

A Tabela 37 pormenoriza os controlos da publicação (Paulsen e Toth, 2016), num total de 36 disposições, das quais, 18 do tipo Administrativo e igualmente do tipo Técnico. Trinta ocupam uma função Preventiva, somente uma, pertence ao campo Detetivo, e cinco enquadram-se em ações Corretivas. Os controlos estão balizados em 16 das 20 famílias possíveis e as três propriedades CIA predominam. O documento valoriza igualmente os aspetos técnicos e organizacionais.

Tabela 37: Portfólio de Controlos US.NIST.SBIS.TF

Id	Nome	Objetivo	Racionalidade		T	F	Prop	Do	MMC	Referências
			Riscos	Ameaças						
1.6.26	Identificar a Informação Armazenada e Utilizada	Proteger a informação de maior valor para o negócio e outras partes interessadas.	11,12,13 (. . .)	10,21,28 (. . .)	Adm	P	CIA	6	Caótico	Ref
1.3.27	Determinar o valor da informação	Quão crítica os diferentes tipos de informação são para a continuidade operacional do negócio.	10,11,21 (. . .)	14,30,35 (. . .)	Adm	P	CIA	3	Caótico	Ref
1.6.28	Elaborar um Inventário de Informação	Repositório de informação com valor para o negócio.	18,19,21 (. . .)	1,10,30 (. . .)	Adm	P	CIA	6	Caótico	Ref
1.3.29	Compreender as Ameaças e Vulnerabilidades do Negócio	Identificar estratégias de proteção contra determinada ameaça ou vulnerabilidade.	1,7,8 (. . .)	19,35,46 (. . .)	Adm	P	CIA	3	Caótico	Ref
1.5.30	Identificar e Controlar quem tem acesso à Informação de Negócio	Proteger a informação de acessos, exfiltração e divulgação não autorizadas.	11,16,20 (. . .)	31,38,42 (. . .)	Adm	P	CIA	5	Caótico	Ref
1.18.31	Realizar Verificação de Antecedentes	Identificar possível usurpação de identidade e assegurar elegibilidade para a função.	11,16,17 (. . .)	14,35,41 (. . .)	Adm	P	CIA	18	Caótico	Ref
1.9.32	Exigir Contas de Utilizador Individuais para Cada Colaborador	Investigar perda de informação ou manipulação não autorizada de dados.	18,20,21 (. . .)	7,10,37 (. . .)	Adm	P	CIA	9	Caótico	Ref
1.12.33	Criar Políticas e Procedimentos de Segurança da Informação	Identificar práticas aceitáveis e expectativas para as operações de negócio.	2,8,9 (. . .)	11,38,46 (. . .)	Adm	P	CIA	12	Caótico	Ref
1.5.34	Limitar o Acesso do Colaborador a Dados e Informação	Prevenir o acesso não autorizado a dados e informação.	14,18,21 (. . .)	42,43,45 (. . .)	Adm	P	CIA	5	Caótico	Ref
1.11.35	Instalar Supressores de Pico de Tensão e Fontes de Alimentação Ininterrupta	Proteção contra alterações e falhas de corrente elétrica.	5,13,19 (. . .)	8,16,34 (. . .)	Tec	P	CIA	11	Caótico	Ref
1.11.36	Atualização de Sistemas Operativos e Aplicações	Diminuir a superfície de ataque.	21,18,22 (. . .)	10,15,27 (. . .)	Tec	P	CIA	11	Caótico	Ref
1.14.37	Instalar e Ativar *Firewalls* de *Software* e *Hardware* em todas as Redes Corporativas	Bloquear tráfego indesejado.	18,19,21 (. . .)	1,10,29 (. . .)	Tec	P	CIA	14	Caótico	Ref
1.14.38	Proteger os Pontos de Acesso sem Fios e as Redes	Assegurar a resiliência dos fluxos de informação nas redes.	10,15,21 (. . .)	14,23,28 (. . .)	Tec	P	CIA	14	Caótico	Ref
1.10.39	Configurar filtros de *Web* e *E-mail*	Evitar correio eletrónico não solicitado e transferência de conteúdos ilícitos.	18,19,21 (. . .)	14,30,39 (. . .)	Tec	P	CIA	10	Caótico	Ref
1.14.40	Usar Criptografia para Informações Confidenciais de Negócio	Proteger o conteúdo da informação armazenada ou em trânsito.	6,11,12 (. . .)	1,22,23 (. . .)	Tec	P	CI	14	Caótico	Ref
1.15.41	Eliminação Segura de Computadores Obsoletos e Suportes de Armazenamento	Evitar a exfiltração de dados empresariais e pessoais.	3,4,5 (. . .)	7,10,12 (. . .)	Tec	P	C	15	Caótico	Ref
1.19.42	Formar os Colaboradores	Assegurar que os colaboradores estão cientes das suas responsabilidades em termos de segurança da informação.	11,16,17 (. . .)	19,33,44 (. . .)	Adm	P	CIA	19	Caótico	Ref
1.10.43	Instalar e Atualizar Programas de Antivírus, *Spyware* e Outros *Anti-malware*	Acautelar o roubo ou dano em dispositivos e programas.	18,21,22 (. . .)	26,28,41 (. . .)	Tec	P	CIA	10	Caótico	Ref
1.2.44	Manter e Monitorizar os Registos	Identificar atividade suspeita e auxiliar em caso de investigação.	15,18,21 (. . .)	30,45,46 (. . .)	Tec	D	CIA	2	Caótico	Ref
1.17.45	Desenvolver um Plano para Desastres e Incidentes de Segurança da Informação	Criar um plano que enumere as ações a executar, em caso de um fogo, emergência médica, arrombamento/assalto, ou desastre natural.	6,15,20 (. . .)	11,35,46 (. . .)	Adm	C	CIA	17	Caótico	Ref
1.13.46	Concretizar Cópias de Segurança Completas de Dados / Informações de Negócio Importantes	Restaurar dados no caso de avaria de um computador, erro humano, ou um programa malicioso infetar o sistema.	11,12,14 (. . .)	15,20,30 (. . .)	Tec	C	A	13	Caótico	Ref
1.13.47	Efetuar Cópias de Segurança Incrementais de Dados / Informações de Negócio Importantes	Restaurar dados no caso de avaria de um computador, erro humano, ou um programa malicioso infetar o sistema.	11,12,14 (. . .)	15,20,30 (. . .)	Tec	C	A	13	Caótico	Ref
1.17.48	Considerar um Seguro de Cibersegurança	Poder ajudar a responder e recuperar de um incidente de segurança.	5	11.19	Adm	C	CIA	17	Caótico	Ref
1.7.49	Realizar Melhorias a Processos / Procedimentos / Tecnologias	Avaliar, corrigir e aperfeiçoar os processos, procedimentos e tecnologias segundo os riscos identificados.	1,8,20 (. . .)	11,35,46 (. . .)	Adm	C	CIA	7	Caótico	Ref
1.18.50	Prestar Atenção às Pessoas do Trabalha e em Redor	Vigiar atividades invulgares ou sinais de aviso, tais como, um colaborador ou prestador de serviços, começar a trabalhar a horas estranhas.	5,6,21 (. . .)	1,7,13 (. . .)	Adm	P	CIA	18	Caótico	Ref
1.19.51	Ter Cuidado com os Anexos de *E-mail* e as ligações *Web*	Evitar disrupção e exfiltração de informação através de programas maliciosos.	10,19,21 (. . .)	1,14,26 (. . .)	Adm	P	CIA	19	Caótico	Ref
1.12.52	Utilizar Computadores, Dispositivos Móveis e Contas Pessoais e Corporativas Separadas	Diminuir a superfície de ataque, por os ativos pessoais à partida serem menos seguros, e evitar violações de dados pessoais.	15,18,21 (. . .)	30,32,46 (. . .)	Adm	P	CIA	12	Caótico	Ref
1.15.53	Não Conectar Dispositivos Pessoais ou de Armazenamento não Confiáveis, ou *Hardware* no Computador, Dispositivo Móvel, ou Rede Corporativa	Conter a propagação de *malware*.	10,18,21 (. . .)	21,22,27 (. . .)	Tec	P	CIA	15	Caótico	Ref
1.10.54	Tomar Precauções na Transferência de *Software*	Evitar falta de suporte e funcionalidades nos programas, assim como propagação de código malicioso.	15,18,19 (. . .)	26,29,32 (. . .)	Tec	P	CIA	10	Caótico	Ref
1.19.55	N Fornecer informações Pessoais ou de Negócio	Precaver divulgação de informação pessoal ou de negócio a atores maliciosos.	3,5,6 (. . .)	39,42,43 (. . .)	Adm	P	C	19	Caótico	Ref
1.10.56	Estar Atento aos *Pop-ups* Nocivos	Prevenir programas maliciosos de infetarem o dispositivo.	6,10,21 (. . .)	26,30,32 (. . .)	Tec	P	CIA	10	Caótico	Ref
1.9.57	Usar Palavras-passe Fortes	Acautelar exfiltração de segredos, por ataques de força bruta entre outras técnicas.	18,21,22 (. . .)	37,39,41 (. . .)	Tec	P	CIA	9	Caótico	Ref
1.14.58	Conduzir Negócios *On-line* de Modo mais Seguro	Prevenir o roubo de informações importantes no caso do sistema ser comprometido.	5,8,12 (. . .)	3,10,23 (. . .)	Tec	P	CIA	14	Caótico	Ref
1.8.59	Subcontratar Serviços Tecnológicos e de Segurança da Informação	Garantir que o serviço contratado vai ao encontro das expectativas, em termos de nível de serviço e segurança.	2.7	19.35	Adm	P	CIA	8	Caótico	Ref
1.3.60	Executar Varredura de Vulnerabilidades	Determinar ativos vulneráveis e sem a totalidade das atualizações instaladas.	18,21,22 (. . .)	1,10,23 (. . .)	Tec	P	CIA	8	Caótico	Ref
1.3.61	Conduzir Teste de Intrusão	Avaliar a possibilidade da rede corporativa, dispositivos, aplicações e pessoas serem alvo de exploração.	3,20,21 (. . .)	14,29,45 (. . .)	Tec	P	CIA	8	Caótico	Ref

Legenda: Id - Identificador | T - Tipo [Adm - Administrativo, Tec - Técnico] | F - Função [P - Preventivo, D - Detetivo, C - Corretivo,] | Prop - Propriedades | Do - Domínios | Ref - US.NIST.SBIS.TF

O catálogo de ações, referentes aos exercícios anteriormente relatados, estendem-se da Tabela 38 à 73. Observam-se 68 métricas de avaliação, para o conjunto de 36 controlos desta publicação. Existem 19 ações enquadradas no perfil Definido e sete no Otimizado. Vinte e três ações são rotuladas como “Recomendado”, duas “Alternativa” e uma “Complemento”.

Tabela 38: Identificar a Informação Armazenada e Utilizada

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.6.26	Identificar a Informação Armazenada e Utilizada	1	Identificar que informação é mais valiosa para o negócio ou outras partes interessadas.	-	1. Número de tipos de informação identificados. 2. Número de partes interessadas envolvidas na identificação da informação.	Df	R	N
		2	Listar todos os tipos de informação utilizados e armazenados pelo negócio.	-		Df		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 39: Determinar o valor da informação

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.3.27	Determinar o valor da informação	1	Indagar para cada conjunto de tipo de informação identificado: (i) O que acontece ao negócio, se a informação é divulgada publicamente?; (ii) O que acontece ao negócio, se a informação está incorreta?; (iii) O que acontece ao negócio, se a informação não está acessível aos colaboradores ou clientes?; (iv) Qual o impacto em termos de reputação para o negócio?; (v) Qual o impacto em termos de produtividade?; (vi) Qual o impacto em termos de responsabilidades legais?.	-	1. % de conjuntos de tipo de informação classificados.	Df	R	N
		2	Classificar o quão crítico cada tipo de informação é, para as operações contínuas do negócio e definir uma classificação geral ou pontuação de risco.	-		Df		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 40: Elaborar um Inventário de Informação

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.6.28	Elaborar um Inventário de Informação	1	Identificar a tecnologia, i.e., *hardware* e *software*, usada para armazenar, aceder, processar e transmitir os diversos tipos de informação.	-	1. Número de categorias de informação e tecnologias associadas, registadas no inventário. 2. % de categorias de informação e tecnologias com responsáveis definidos.	Df	R	N
		2	Incluir a marca, modelo, números de série, e outras informações de identificação.	-		Nc		N
		3	Todos os tipos de informação devem ter, pelo menos, uma tecnologia de *hardware* / *software* listada. Quando aplicável, incluir tecnologias fora do negócio (por exemplo, "a nuvem") e quaisquer tecnologias de proteção existentes, tais como *firewalls*.	-		Nc		N
		4	Rastrear a localização de cada tipo de informação.	-		Nc		N
		5	Associar o dono da tecnologia, se aplicável.	-		Nc		N
		6	Determinar o impacto global potencial da informação.	-		Df		N
		7	Atualizar o inventário, pelo menos anualmente.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 41: Compreender as Ameaças e Vulnerabilidades do Negócio

Identificador	Nome	It	Ações	OdA	Métricas	Perfil	Entregáveis	R
1.3.29	Compreender as Ameaças e Vulnerabilidades do Negócio	1	Identificar estratégias específicas de proteção contra ameaças ou vulnerabilidades, através da revisão regular das ameaças e vulnerabilidades, que podem afetar o negócio e estimar a *likelihood* de afetação dessa ameaça ou vulnerabilidade.	-	1. Contagem de ameaças e vulnerabilidades identificadas. 2. Número de ameaças e vulnerabilidades assinaladas no último ano.	Df	V	N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 42: Identificar e Controlar quem tem acesso à Informação de Negócio

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.5.30	Identificar e Controlar quem tem acesso à Informação de Negócio	1	Determinar quem deve ter acesso à informação de negócio e se uma chave, privilégio administrativo ou palavra-passe é necessária.	-	1. % de utilizadores com acessos e privilégios mapeados, face aos sistemas e aplicações da empresa. 2. % de instalações com controlo de acessos físicos implementados. 3. Número de dispositivos móveis com cadeado. 4. Soma dos ecrãs com tela de privacidade.	Nuclear	S	N
		2	Não permitir desconhecidos ou pessoas não autorizadas, a terem acesso físico a qualquer um dos computadores empresariais. Inclui pessoal de limpeza e manutenção.	-		Nuclear		N
		3	Não permitir pessoal de reparação de computadores ou rede, trabalhar em sistemas ou dispositivos sem supervisão.	-		Nuclear		N
		4	Nenhuma pessoa não reconhecida, deve poder entrar no espaço de escritório, sem ser questionada por um funcionário.	-		Nuclear		N
		5	Trancar fisicamente os computadores portáteis e outros dispositivos móveis, quando não estão a ser utilizados.	-		Ot		N
		6	Utilizar a funcionalidade de bloqueio de sessão, incluída em nos sistemas operativos, que bloqueia o ecrã, se o computador não for utilizado durante um período de tempo especificado (por exemplo, 2 minutos).	-		Nuclear		N
		7	Utilizar um ecrã de privacidade ou posicionar a tela de cada computador, para não se conseguir ver a informação no ecrã, por quem passe nas proximidades.	-		Nuclear		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 43: Realizar Verificação de Antecedentes

Identificador	Nome	It	Ações	OdA	Métricas	P	E	R
1.18.31	Realizar Verificação de Antecedentes	1	Fazer uma verificação completa, nacionalmente, dos antecedentes criminais, infrações sexuais e, se possível, responsabilidades de crédito, de todos os potenciais empregados (especialmente se vão manusear fundos empresariais); escolas frequentadas, grau académico, data de graduação, média académica e referências.	-	1. % de colaboradores com verificação de antecedentes efetuado. 2. Número de candidatos não admitidos, pela verificação de antecedentes realizado.	Nuclear	U	N
		2	Considerar cada colaborador conduzir uma verificação de antecedentes.	Recomendado		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 44: Exigir Contas de Utilizador Individuais para Cada Colaborador

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.9.32	Exigir Contas de Utilizador Individuais para Cada Colaborador	1	Criar contas separadas para cada utilizador, incluindo prestadores de serviço, que necessitem de acesso.	-	1. Número de contas privilegiadas existentes. 2. Soma de contas genéricas em utilização. 3. Contagem de senhas fracas em uso.	Nuclear	S	N
		2	Requerer palavras-passe fortes e únicas para cada conta.	-		Nc		N
		3	Assegurar que todos os colaboradores utilizam contas informáticas, sem privilégios administrativos, para desempenhar funções de trabalho típicas.	-		Nc		N
		4	Considerar a utilização de uma conta convidada com privilégios mínimos (por exemplo, apenas acesso à Internet), se necessário para o negócio.	Recomendado		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 45: Criar Políticas e Procedimentos de Segurança da Informação

Identificador	Nome	It	Ações	OdA	Métricas	P	E	R
1.12.33	Criar Políticas e Procedimentos de Segurança da Informação	1	As políticas e procedimentos de segurança da informação e cibersegurança, devem descrever as expectativas para proteger as informações e sistemas; identificar os recursos e informações importantes; a perspetiva da gestão em relação ao uso e proteção dos recursos por parte dos colaboradores; e enumerar as práticas aceitáveis e expectativas para as operações de negócio.	-	1. % de colaboradores sensibilizados e consciencializados em relação às políticas e procedimentos da organização. 2. Número de políticas e procedimentos em vigor na empresa. 3. Número de processos disciplinares levantados por incumprimento do estipulado nas políticas corporativas. 4. % de políticas revistas pelo departamento jurídico. 5. % de políticas revistas anualmente.	Nuclear	W	N
		2	Estarem acessíveis a todos os colaboradores (e.g., manual do funcionário).	-		Nc		N
		3	Ter um profissional jurídico familiarizado com a legislação cibernética, a rever as políticas para assegurar, que estão conforme as leis locais e regulamentos.	-		Df		N
		4	Assinar uma declaração, por parte dos colaboradores, em que concordam ter lido e vão seguir, as políticas e procedimentos relevantes.	-		Nc		N
		5	Rever, atualizar pelo menos anualmente e sempre que hajam alterações na organização ou tecnologia empregue.	-		Nc		N
		6	Tomar conhecimento de alterações às políticas, por parte dos colaboradores, e compreensão das mesmas, por assinatura.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 46: Limitar o Acesso do Colaborador a Dados e Informação

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.5.34	Limitar o Acesso do Colaborador a Dados e Informação	1	Restringir o acesso a sistemas e informação, ao mínimo necessário, à execução das tarefas corporativas, por parte de cada utilizador.	-	1. Número de funções criadas em cada aplicação, com privilégios definidos, que mapeiam a estrutura organizacional. 2. % de colaboradores com o processo de saída concluído, face ao número total de saídas.	Nuclear	S	N
		2	Impossibilitar, que somente um indivíduo, incluíndo executivos e gestores séniores, inicie e aprove uma transação, seja ela financeira ou outra.	-		Nc		N
		3	Assegurar, na saída de um colaborador, que o mesmo não tenha mais acesso à informação de negócio e a sistemas.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 47: Instalar Supressores de Pico de Tensão e Fontes

Identificador	Nome	It	Ações	OdA	Métricas	P	E	R
1.11.35	Instalar Supressores de Pico de Tensão e Fontes de Alimentação Ininterrupta	1	Assegurar que cada computador e dispositivos críticos de rede estão conectados a uma UPS.	-	1. % de dispositivos críticos ligados a uma UPS. 2. % de dispositivos sem qualquer proteção contra falhas de corrente elétrica.	Nuclear	X	N
		2	Ligar dispositivos não críticos a supressores de pico de tensão.	-		Nc		N
		3	Testar e trocar as UPS e os supressores de pico de tensão consoante as recomendações do fabricante.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 48: Atualização de Sistemas Operativos e Aplicações

Identificador	Nome	It	Ações	OdA	Métricas	P	E	R
1.11.36	Atualização de Sistemas Operativos e Aplicações	1	Atualizar e corrigir todo o *software*, em cada dispositivo corporativo.	-	1. Número de aplicações obsoletas ainda em uso. 2. Número de sistemas ou aplicações com atualizações não programadas, pelo menos mensalmente.	Nuclear	M	N
		2	Instalar somente as aplicações necessários ao negócio.	-		Nc		N
		3	Ter apenas *software* com versão atualizada e suportada pelo fabricante.	-		Nc		N
		4	Na aquisição de novos computadores ou *software*, verificar se existem atualizações de imediato.	-		Nc		N
		5	Assignar um dia por mês, para procurar atualizações.	Recomendado		Nc		N
		6	Usar um produto que varra os sistemas e notifique caso haja atualizações necessárias.	Recomendado		Df		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 49: Instalar e Ativar *Firewalls* de *Software* e *Hardware*

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.14.37	Instalar e Ativar *Firewalls* de *Software* e *Hardware* em todas as Redes Corporativas	1	Instalar e operar uma *firewall* de *hardware* entre a rede interna e a *internet*.	-	1. % de telemóveis inteligentes com *firewall* gerida. 2. % de computadores onde os registos da *firewall* de *software* foram analisados no último ano.	Nuclear	D	N
		2	Garantir a existência de *software* antivírus instalado na *firewall*.	-		Nc		N
		3	Alterar a palavra-passe de administração por defeito e regularmente.	-		Nc		N
		4	Mudar o nome de *login* da conta de administração.	Recomendado		Nc		N
		5	Instalar, usar e atualizar regularmente, uma *firewall* de *software* em todos os computadores, telemóveis e em outros dispositivos de rede, sempre que tecnicamente viável, mesmo que esteja em uso uma VPN ou um prestador de serviços nuvem.	-		Otimizado		N
		6	Habilitar o registo nas *firewalls* de *software*.	-		Nc		N
		7	Utilizar somente uma versão da *firewall* de *hardware* ou *software*, que seja atualizável, autêntica, e suportada pelo fabricante.	-		Nc		N
		8	Assegurar que o trabalho prestado a partir de casa, também está protegido pelo uso de *firewalls* por *hardware* e *software*.	-		Df		N
		9	Instalar um IDPS na rede corporativa.	Recomendado		Df		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 50: Proteger os Pontos de Acesso sem Fios e as Redes

Identificador	Nome	It	Ações	OdA	Métricas	P	E	R
1.14.38	Proteger os Pontos de Acesso sem Fios e as Redes	1	Alterar a palavra-passe de administração por defeito no dispositivo.	-	1. Número de utilizadores com ligação VPN configurada.	Nuclear	Y	N
		2	Desabilitar a funcionalidade de transmissão do SSID.	-		Nc		N
		3	Configurar o *router* para utilizar o protocolo WPA-2 com AES.	-		Nc		N
		4	Assegurar que o acesso *internet* sem fios providenciado aos clientes, é separado do da rede corporativa.	-		Nc		N
		5	Aceder somente a redes sem fios detidas ou confiáveis.	-		Nuclear		N
		6	Implementar uma VPN em caso de necessidade de ligação a uma rede desconhecida ou trabalhar a partir de casa.	Recomendado		Nuclear		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 51: Configurar filtros de *Web* e *E-mail*

Identificador	Nome	It	Ações	OdA	Métricas	P	E	R
1.10.39	Configurar filtros de *Web* e *E-mail*	1	Utilizar filtragem de *malware* nos anexos e conteúdos não solicitados.	-	1. Número de mensagens de correio eletrónico ou páginas *web*, bloqueadas no último mês.	Nuclear	K	N
		2	Habilitar a função de filtragem de páginas *web*.	-		Nc		N
		3	Bloquear *websites* associados a ameaças de cibersegurança (e.g., pornografia).	Recomendado		Nc		N
		4	Configurar as *firewalls* ou *routers* para bloquear certos blocos de endereços (*blacklist*) ou apenas permitir certos endereços (*whitelist*).	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 52: Usar Criptografia para Informações Confidenciais de Negócio

Identificador	Nome	It	Ações	OdA	Métricas	P	E	R
1.14.40	Usar Criptografia para Informações Confidenciais de Negócio	1	Cifrar a totalidade dos discos — que encripta toda a informação nos meios de armazenamento — em todos os computadores, *tablets*, e telefones inteligentes.	-	1. % de dispositivos móveis cifrados.	Nuclear	Z	N
		2	Guardar uma cópia da palavra-passe de encriptação ou chave, numa localização segura e separado do local onde as cópias de segurança são armazenadas.	-		Nc		N
		3	Encriptar o enviar documentos ou *e-mails* sensíveis.	Recomendado		Nc		N
		4	Enviar senhas ou chaves, por outro canal de comunicação, ao usado na transmissão da informação (e.g., envio de mensagem de correio eletrónica cifrada, a senha de desencriptação transmitir por telefone).	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 53: Eliminação Segura de Computadores Obsoletos e Suportes de Armazenamento

Identificador	Nome	It	Ações	Opções das Ações	Métricas	P	E	R
1.15.41	Eliminação Segura de Computadores Obsoletos e Suportes de Armazenamento	1	Limpar eletronicamente os discos rígidos.	Alternativa	1. % de suporte de dados, objeto de um processo seguro de destruição. 2. Número de trituradores de papel na organização.	Nuclear		N
		2	Desmagnetizar os discos rígidos.			Df		N
		3	Destruir fisicamente os discos rígidos.	-		Nc		N
		4	Escolher uma empresa de destruição de discos, que permita observar o processo.	Recomendado		Df	Y	N
		5	Instalar uma aplicação de limpeza remota nos computadores, *tablets*, telemóveis, e outros dispositivos móveis.	-		Df		N
		6	Na eliminação de suporte de dados antigos (e.g., CD, disquetes, USB), primeiro eliminar os dados de negócio sensíveis ou pessoais. A seguir destruir o suporte por trituração.	-		Nc		N
		7	Na erradicação de papéis com informação sensível, usar um triturador de papel.	-		Nc		N
		8	Incinerar papéis e outros suportes de dados, que contenham informação muito sensível.	Recomendado		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 54: Formar os Colaboradores

Identificador	Nome	It	Ações	OdA	Métricas	P	E	R
1.19.42	Formar os Colaboradores	1	Formar os utilizadores imediatamente quando contratados e pelo menos uma vez por ano, posteriormente, sobre as políticas de segurança da informação e o que se espera que façam para proteger a informação e tecnologia do negócio.	-	1. Número de utilizadores formados nos trinta posteriores à assinatura do contrato de trabalho. 2. Número de utilizadores avaliados, após receberem sensibilização em segurança da informação.	Nuclear	J	N
		2	Assegurar que assinam uma declaração, onde se comprometem a seguir as políticas instituídas, e que compreendam as penalidades em caso contrário.	-		Nc		N
		3	Incluir nos treinos, cenários de emergência ou incidentes de segurança, como tratar a informação dos clientes e de negócio, e de que modo se podem usar os computadores e telemóveis corporativos.	-		Nc		N
		4	Reforçar continuamente a formação nas conversas ou reuniões do dia a dia.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 55: Instalar e Atualizar Programas de Antivírus, *Spyware* e Outros *Anti-malware*

Identificador	Nome	It	Ações	OdA	Métricas	P	E	R
1.10.43	Instalar e Atualizar Programas de Antivírus, *Spyware* e Outros *Anti-malware*	1	Instalar, utilizar e atualizar regularmente os programas antivírus e *anti-spyware*, em todos os dispositivos utilizados no negócio (incluindo computadores, telemóveis inteligentes e *tablets*).	-	1. % de dispositivos com programas *anti-malware* instalados. 2. Número de dispositivos com avisos ativos de *malware* há mais de trinta dias?	Nuclear	K	N
		2	Verificar a existência de atualizações, pelo menos diariamente, ou em tempo real, se possível, e executar uma varredura completa logo a seguir.	-		Nc		N
		3	Execução de trabalho corporativo a partir de equipamentos pessoais, requer o uso de software *anti-malware*.	-		Nc		N
		4	Utilizar duas soluções antivírus de fabricantes diferentes.	Recomendado		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 56: Manter e Monitorizar os Registos

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.2.44	Manter e Monitorizar os Registos	1	Assegurar que a funcionalidade de registo de atividades, está ativa nos sistemas de *hardware* e *software*, de proteção / deteção (e.g., *firewalls*, antivírus).	-	1. % de sistemas e dispositivos com a funcionalidade de *logs* ativa. 2. % de sistemas e dispositivos com cópias de segurança nos registos. 3. Mediana de retenção dos registos.	Nuclear	Q	N
		2	Os registos devem ser alvo de cópia de segurança e guardados, no mínimo, um ano; alguns tipos de informação podem ter de ser retidos por um período não inferior a seis anos (e.g., registos clínicos de pacientes).	-		Nc		N
		3	Haver um profissional de cibersegurança, que reveja os registos, à procura de tendências invulgares ou indesejadas.	Recomendado		Otimizado		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 57: Desenvolver um Plano para Desastres e Incidentes de Segurança da Informação

Identificador	Nome	It	Ações	OdA	Métricas	P	E	R
1.17.45	Desenvolver um Plano para Desastres e Incidentes de Segurança da Informação	1	Definir papéis e responsabilidades.	-	1. Número de categorias de incidentes de segurança tipificados? 2. Número de incidentes de segurança da informação registados nos últimos três meses?	Nuclear	X	N
		2	Determinar o que fazer com os dados e o sistemas de informação, em caso de incidente.	-		Nc		N
		3	Delinear quem chamar em caso de um incidente.	-		Nc		N
		4	Decidir os tipos de atividades, que constituem um incidente de segurança da informação.	-		Nc		N
		5	Desenvolver procedimentos para cada função, que descreva exatamente o que é esperado de cada indivíduo naquela posição, num incidente ou emergência.	Recomendado		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 58: Concretizar Cópias de Segurança Completas de Dados / Informações de Negócio Importantes

Identificador	Nome	It	Ações	OdA	Métricas	P	E	R
1.13.46	Concretizar Cópias de Segurança Completas de Dados / Informações de Negócio Importantes	1	Realizar uma cópia de segurança completa e encriptada dos dados em cada computador e dispositivo móvel utilizado no negócio, pelo menos uma vez por mês, pouco depois de uma varredura completa do antivírus.	-	1. % de salvaguardas com cópias numa outra localização física ou num prestador de serviços na nuvem? 2. % de cópias de segurança encriptadas? 3. Tempo de retenção de cada conjunto de dados guardados? 4. Taxa de *backups* restaurados com sucesso?	Nuclear	O	N
		2	Armazenar as cópias de segurança, numa localização diferente da do edifício, onde se realizam as salvaguardas.	-		Nc		N
		3	Guardar uma cópia da senha ou chave de encriptação, num local seguro e separado do local onde se encontram as cópias de segurança armazenadas.	-		Nc		N
		4	Encriptar todos os dados, antes de salvaguardar as cópias num prestador de serviços na nuvem.	Recomendado		Nc		N
		5	Reter as cópias de segurança por um ano.	-		Nc		N
		6	Testar as cópias de segurança, imediatamente após a sua criação.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 59: Efetuar Cópias de Segurança Incrementais de Dados / Informações de Negócio Importantes

Identificador	Nome	It	Ações	OdA	Métricas	P	E	R
1.13.47	Efetuar Cópias de Segurança Incrementais de Dados / Informações de Negócio Importantes	1	Conduzir um *backup* automático incremental ou diferencial de cada um dos computadores e dispositivos móveis corporativos, pelo menos uma vez por semana.	-	1. % de salvaguardas com cópia para a nuvem? 2. % de cópias de segurança encriptadas? 3. Tempo de retenção de cada conjunto de dados guardados? 4. Taxa de *backups* restaurados com sucesso?	Nuclear	O	N
		2	Armazenar as cópias de segurança, em suporte amovível, num servidor isolado da rede, ou na nuvem.	-		Nc		N
		3	Encriptar os *backups*.	Recomendado		Nc		N
		4	Guardar uma cópia da senha ou chave de encriptação, num local seguro e separado do local onde se encontram as cópias de segurança armazenadas.	-		Nc		N
		5	Reter as cópias de segurança por 52 semanas.	-		Nc		N
		6	Testar as cópias de segurança periodicamente.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 60: Considerar um Seguro de Cibersegurança

Identificador	Nome	It	Ações	OdA	Métricas	P	E	R
1.17.48	Considerar um Seguro de Cibersegurança	1	Determinar os riscos da organização antes de adquirir uma apólice.	-	1. Número de riscos identificados? 2. Número de companhias de seguros avaliadas no último ano?	Nuclear	V	N
		2	Avaliar a companhia de seguros que oferece proteção, os serviços prestados, o tipo de eventos cobertos, e assegurar que têm uma boa reputação e conseguem cumprir o acordo contratado.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 61: Realizar Melhorias a Processos / Procedimentos / Tecnologias

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.7.49	Realizar Melhorias a Processos / Procedimentos / Tecnologias	1	Avaliar regularmente os processos, procedimentos e soluções tecnológicas conforme os riscos identificados.	-	1. Número de processos, procedimentos e soluções tecnológicas revistas no ano transato?	Df	D	N
		2	Realizar treinos ou exercícios *table-top*, que simulem ou executem passo a passo um cenário de um evento principal, de modo a identificar potenciais fraquezas nos processos, procedimentos, tecnologia, ou prontidão do pessoal.	Recomendado	2. Número de cenários com simulações executadas?	Otimizado		N
		3	Fazer correções e melhorias, conforme necessário.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 62: Prestar Atenção às Pessoas do Trabalha e em Redor

Identificador	Nome	It	Ações	OdA	Métricas	P	E	R
1.18.50	Prestar Atenção às Pessoas do Trabalha e em Redor	1	Conhecer e manter contacto com todos os utilizadores, incluindo terceiras partes contratadas ou que partilhem as mesmas instalações (e.g., para limpeza, segurança, manutenção).	-	1. Número de incidentes de outras organizações nos últimos cinco anos, localizadas perto da empresa, considerados um possível risco?	Nuclear	J	N
		2	Estar atento a atividade invulgar perto do local de trabalho ou no setor de atividade da organização, inlcluindo a realização de atividades, que possam constituir um risco ambiental ou de segurança.	-	2. Número de contactos com autoridades e grupos de interesse estabelecidos ou subscritos?	Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 63: Ter Cuidado com os Anexos de *E-mail* e as ligações *Web*

Identificador	Nome	It	Ações	Opções das Ações	Métricas	P	E	R
1.19.51	Ter Cuidado com os Anexos de *E-mail* e as ligações *Web*	1	N clicar num *hyperlink* ou abrir um anexo, que não se espera.	Complemento	1. Taxa de utilizadores com formação em *phishing*?	Nuclear	J	N
		2	Telefonar ao remetente para verificar se o *e-mail* foi enviado e pedir a descrição do anexo ou ligação.		2. Número de mensagens de correio eletrónico reportadas por suspeita de textitphishing no último ano?	Nc		N
		3	Formar os indivíduos para reconhecer tentativas de *phishing* e quem notificar quando ocorre.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 64: Utilizar Computadores, Dispositivos Móveis e Contas Pessoais e Corporativas Separadas

Identificador	Nome	It	Ações	OdA	Métricas	P	E	R
1.12.52	Utilizar Computadores, Dispositivos Móveis e Contas Pessoais e Corporativas Separadas	1	Ter dispositivos e contas de correio eletrónico separadas, para assuntos pessoais e de negócio.	-	1. % de colaboradores que usam computadores ou telemóveis pessoais no exercício de atividades empresariais?	Nuclear	J	N
		2	Utilização de um computador separado, que não esteja ligado a qualquer rede, para certas funções empresariais ou para informação extremamente sensível.	Recomendado		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 65: Não Conectar Dispositivos Pessoais ou de Armazenamento não Confiáveis, ou *Hardware* no Computador, Dispositivo Móvel, ou Rede Corporativa

Identificador	Nome	It	Ações	OdA	Métricas	P	E	R
1.15.53	Não Conectar Dispositivos Pessoais ou de Armazenamento não Confiáveis, ou *Hardware* no Computador, Dispositivo Móvel, ou Rede Corporativa.	1	Não partilhar unidades USB ou discos rígidos externos, entre computadores ou dispositivos pessoais e empresariais.	-	1. Número de dispositivos com a funcionalidade de execução automática desligada para os periféricos?	Nuclear	K	N
		2	Não ligar nenhum *hardware* desconhecido, não confiável ao sistema ou rede e não inserir nenhum CD, DVD, ou drive USB desconhecida.	-		Df		N
		3	Desativar a funcionalidade *AutoRun* para as portas USB e unidades óticas, como CD e DVD dos computadores empresariais.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 66: Tomar Precauções na Transferência de *Software*

Identificador	Nome	It	Ações	OdA	Métricas	P	E	R
1.10.54	Tomar Precauções na Transferência de *Software*	1	N descarregar *software* de páginas *web* desconhecidas.	-	1. % de programas *freeware* ou *shareware* em uso, pré-aprovados na organização?	Nuclear	K	N
		2	A transferência e uso de *freeware* ou *shareware* tem de ser avaliada em termos de suporte técnico e funcionalidades disponibilizadas.	-	2. Número de vezes no último ano, que a lista de *websites* visitados pelos utilizadores foi verificada?	Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 67: Não Fornecer informações Pessoais ou de Negócio

Id	Nome	It	Ações	Opções das Ações	Métricas	P	E	R
1.19.55	Não Fornecer informações Pessoais ou de Negócio	1	Ao se receber uma chamada não solicitada, pedindo informação pessoal de uma empresa reconhecida, requerer informação identificativa, que apenas uma pessoa associada a essa organização pode saber.	Alternativa	1. % de pessoas que receberam sensibilização em ataques de engenharia social?	Nuclear	J	N
		2	Ao se receber uma chamada não solicitada, pedindo informação pessoal de uma empresa reconhecida, pedir ao interlocutor o nome e departamento, desligar e retornar a chamada, usando os contactos disponibilizados na página da empresa reconhecida, ou num possível contrato, ou fatura existente, e pedir para falar com o interlocutor. Nunca usar o número ou outra forma de contacto disponibilizada pelo interlocutor.		2. Número de casos reportados ligados a engenharia social? 3. Taxa de incidentes de segurança despoletados tendo como causa raiz a engenharia social?	Nc		N
		3	Em tempo algum, responder a um telefonema não solicitado de uma empresa, que não se reconheça, e peça informações pessoais ou empresariais sensíveis.	-		Nc		N
		4	Os colaboradores devem notificar o superior, sempre que haja uma tentativa ou pedido de informação de negócio sensível.	-		Nc		N
		5	Nunca dar a terceiros, o nome de utilizador ou a palavra-passe, e outro tipo de informações, que facilitem um ataque malicioso (e.g., tipo de SO utilizado, marcas de *firewall*, navegador de *internet*, aplicações instaladas).	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 68: Estar Atento aos *Pop-ups* Nocivos

Identificador	Nome	It	Ações	OdA	Métricas	P	E	R
1.10.56	Estar Atento aos *Pop-ups* Nocivos	1	Usar um bloqueador de *pop-ups* e apenas permiti-los em *websites* confiáveis.	-	1. Número de computadores com bloqueadores de janelas instalados? 2. Quantidade de vezes,onde os registos de páginas de *web* bloqueadas, são objeto de averiguação por parte da equipa de TI ou segurança?	Nuclear	K	N
		2	No caso de uma janela abrir inexplicavelmente no computador, não fechar a mesma, desligar o dispositivo da rede e eliminar o processo do navegador.	-		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 69: Usar Palavras-passe Fortes

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.9.57	Usar Palavras-passe Fortes	1	As boas senhas consistem numa sequência aleatória de letras (maiúsculas e minúsculas), números, e caracteres especiais, e têm pelo menos 12 caracteres.	-	1. % de sistemas e aplicações a obrigar a utilização de segredos complexos?	Nuclear		N
		2	Para sistemas ou aplicações com informações importantes, utilizar múltiplas formas de identificação (chamada autenticação “multifactor” ou “fator duplo”).	-	2. % de sistemas e aplicações a obrigar a utilização de mais do que um fator de autenticação?	Df	I	N
		3	Muitos dispositivos vêm com palavras-passe de administração padrão; estas devem ser alteradas imediatamente aquando da instalação e regularmente a seguir.	-	3. % de dispositivos onde a palavra-passe original foi trocada?	Nc		N
		4	Considerar a possibilidade de configurar os sistemas e dispositivos, para exigir aos utilizadores, que alterem as suas palavras-passe a cada 3 meses, se possível.	-	4. Número de utilizadores com gestor de segredos instalado e mais de cinco senhas introduzidas?	Nc		N
		5	As senhas para dispositivos e aplicações, que lidam com informação empresarial, não devem ser reaproveitadas.	-	5. Número de vezes que cada utilizador acedeu o gestor de senhas no último mês?	Nc		N
		6	Utilizar uma aplicação de gestão de senhas, que cifre todas as palavras-passe armazenadas, utilize uma senha mestra forte, trocada regularmente.	Recomendado		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 70: Conduzir Negócios *Online* de Modo mais Seguro

Identificador	Nome	It	Ações	OdA	Métricas	P	E	R
1.14.58	Conduzir Negócios *Online* de Modo mais Seguro	1	Transações de negócio, comerciais e bancárias em linha, apenas se devem realizar utilizando uma ligação segura.	-	1. % de páginas em linha acedidas pelo protocolo não seguro HTTP? 2. Número de computadores exclusivos para transações financeiras?	Nuclear	J	N
		2	Apagar regularmente a *cache* do navegador *web*, ficheiros temporários da *internet*, *cookies*, e histórico.	-		Nc		N
		3	Ter um computador dedicado, usado somente para transações bancárias, desligado quando não necessário.	Recomendado		Nc		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 71: Subcontratar Serviços Tecnológicos e de Segurança da Informação

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.8.59	Subcontratar Serviços Tecnológicos e de Segurança da Informação	1	Solicitar recomendações ou referência (e.g., parceiros de negócio, associações empresariais).	-	1. Número de serviços subcontratados avaliados no último ano. 2. % de fornecedores qualificados.	Nuclear	J	N
		2	Ter uma lista de ações ou entregáveis a serem alcançados.	-		Nc		N
		3	Verificar a prestação do subcontratado através do grau de satisfação de outros clientes, queixas ocorridas, tempo em atividade e alterações societárias.	-		Nc		N
		4	Indagar as qualificações, certificações e experiência relevante dos profissionais, a executar as tarefas.	-		Nc		N
		5	Pedir a contribuição ou participação na seleção do subcontratado, a parceiros de negócio ou clientes, que dependam da organização.	Recomendado		Df		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 72: Executar Varredura de Vulnerabilidades

Identificador	Nome	It	Ações	OdA	Métricas	Perfil	Entregáveis	R
1.3.60	Varredura de Vulnerabilidades	1	Conduzir uma análise ou varredura de vulnerabilidades por um profissional, pelo menos anualmente, e sempre que haja alterações substanciais nos computadores e rede.	-	1. Soma das varreduras de rede efetuadas no último ano. 2. % de vulnerabilidades existentes na rede, com mais de noventa dias. 3. Número de vulnerabilidades por ativo crítico.	Df	F	N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

Tabela 73: Conduzir Teste de Intrusão

Id	Nome	It	Ações	OdA	Métricas	P	E	R
1.3.61	Conduzir Teste de Intrusão	1	Conduzir um teste de intrusão contra interesses corporativos.	Recomendado	1. Número de testes de intrusão efetuados no último ano. 2. % de vulnerabilidades remediadas, resultantes do último teste de intrusão. 3. Número de vulnerabilidades não mitigadas, desde a execução do primeiro teste de intrusão.	Otimizado	F	N
		2	O teste de intrusão deve incluir ataque: (i) Físico; (ii) Engenharia social; (iii) Cibernético.	Recomendado		Otimizado		N

Legenda: Id - Identificador | It - Item | OdA - Opções das Ações [Alt - Alternativa , Com - Complemento , Rec - Recomendado] | P - Perfil [Df - Definido , Nc - Nuclear , Ot - Otimizado] | E - Entregáveis | R - Realizado [N - Não]

4.3 ROTEIRO DE MATERIALIZAÇÃO

A Figura 18 corporiza a ordem de realização dos controlos, na ótica do autor. Evidentemente, o leitor, não está subordinado a tal arrumação, sendo livre de reacomodar as atividades da forma que melhor entender. O importante é objetivar as ações dos controlos na organização.
O roteiro de materialização é tendencialmente infinito, na procura da melhoria contínua. Uma primeira iteração na universalidade dos controlos, à partida, não deixará a organização, num estado de maturidade "Aperfeiçoado". Sendo, portanto, necessário a sua contínua reiteração. Mesmo nos casos infrequentes, de se conseguir a plenitude do nível de capacitação na totalidade dos controlos, a recolha e avaliação das métricas é perpétua.

A disposição alvitrada tem subjacente primeiramente as pessoas, posteriormente as tecnologias e por fim os processos. As pessoas, no princípio, por serem "o elo mais fraco em muitas arquiteturas de segurança em ambiente cibernético" (Ferreira, 2021) e "uma das medidas de segurança mais eficazes que uma organização pode tomar é treinar o seu pessoal e criar uma «cultura consciente da segurança»" (Silva, 2023). Ulteriormente entra a parafernália dos controlos técnicos, sendo imperiosos à segurança da organização, por não estarem sujeitos a erros humanos e processuais: "muitos colaboradores não seguem as políticas de segurança recomendadas pela empresa" (Silva, 2023). A concluir o roteiro aparecem os processos, que legislam, as políticas, a sua aplicação e o sistemas normativo da organização. Por "o ser humano também está sujeito a falhas, a decisões erradas, a interpretações duvidosas que podem levar, ou contribuir, para o acidente" (Bordini, 1999), depositar-se demasiada crença nos processos é um erro. O fundamento de um programa resiliente de cibersegurança para as PME é assentar vigorosamente nas pessoas, agudamente em medidas de mitigação tecnológica e brandamente nos processos. Uma ponderação cuidadosa à Figura 18 permite vislumbrar a exposição precedente.

Figura 18: Roteiro de Materialização

Embora os 61 controlos e as 275 ações derivadas possam configurar um juízo de quantidade assinalável, conforme ilustrado na Figura 19, a amostra necessita de mais dados para se encetar uma eficiente integração de controlos similares.

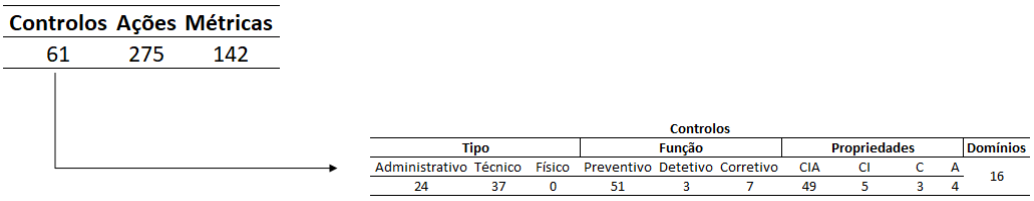


Figura 19: Apuramento Estatístico dos Controlos

Ou seja, deve-se arrumar e aprimorar as ações de críveis controlos filhos sob um controlo pai. O verbo "Arrumar" significa a união de dois ou mais conjuntos em concordância com a teoria dos conjuntos, enquanto o "aprimorar" denota corrigir duplicações, subclasses e outras disfuncionalidades similares. Assim, até ao sequenciamento de uma dezena de *frameworks*, o *Roteiro de Materialização* prolongar-se-à sem demarcações adicionais às atualmente já empregues.

Os anexos D a Z suportam a realização do Roteiro de Materialização, traduzindo as ações dos controlos nos entregáveis (e.g., ferramentas, *softwares*, funcionalidades, documentação) necessários à sua efetivação e evidenciação.

4.4 OUTRAS NORMAS

As secções precedentes corroboram os princípios e objetivos definidos para a dissertação. O trabalho em causa é incontável, pelas inúmeras *frameworks*, normas e publicações relacionados com a temática. O princípio fica sobejamente demonstrado e não se intenta sujeitar o leitor com controlos, ações e outras alegações adicionais. Aplicando a mesma metodologia, a introdução de requisitos adicionais, é não mais, que uma nova iteração ao processo descrito.

Uma inquirição plausível, é o porquê destas três normas e não outras. Além dos motivos supramencionados, ao longo dos segmentos normativos específicos, existe um de ínfero fervor académico, mas possivelmente, de maior arrebatamento para o autor, é por o mesmo nunca se ter debruçado sobre as *frameworks* em causa. Por outro lado, o conjunto dos três documentos comungam de predicados, que materializam o intento da criação do manual prático de cibersegurança e temáticas afins, para as PME. O primeiro enfatiza somente requisitos práticos relevantes. O segundo sustenta controlos pragmáticos, baseados nos incidentes de segurança periquitados ao longo

do ano transato. O terceiro proporciona, além de uma componente técnica objetiva, um firmamento de controlos de índole administrativo, imperiosos na edificação de políticas e processos de avaliação de riscos, fundamentais para as organizações que almejam granjear os perfis "Definido" e "Otimizado".

5

CENÁRIO PRÁTICO

A legitimação empírica do Manual Prático para PME, é objetivada com recurso à avaliação de uma implementação numa empresa[1] de média dimensão, líder no segmento de mercado em que atua. A empresa tem como objeto social a área da consultadoria de soluções integradas num dos ERP de referência nacional. O parque de clientes ultrapassa os mil, a equipa de consultores uma centena, possui projetos numa dezena de países, com múltiplos centros de operações de norte a sul do país e ilhas. O leque de soluções oferecidas abarca, além da consultadoria, outras vertentes, destacando-se o desenvolvimento *web* e aplicações móveis. A materialização do cenário consubstancia os seguintes estágios:

- Apresentação do projeto ao CEO e permissão à condução dos trabalhos;
- Diagnóstico do estado de maturidade através da resposta às ações dos controlos, por parte do responsável de TI;
- Avaliação das respostas obtidas;
- Exposição dos resultados ao conselho de administração.

5.1 APRESENTAÇÃO DO PROJETO

Em reunião com o CEO da organização em causa, observaram-se várias temáticas, nomeadamente:

- Objetivo de realizar a avaliação de maturidade das PME em torno dos assuntos de cibersegurança, segurança da informação, privacidade e proteção de dados pessoais;
- A empresa conseguir obter conhecimento sobre o seu estado de maturidade, um relatório acerca dos pontos fundamentais onde deverá alocar os recursos na proteção do negócio (e dos clientes) e alguns *quick wins*;

1 Nota do autor: a empresa em causa solicita o anonimato, nem pode ser de outra forma, pela exposição a terceiros, que a dissertação em causa obriga. Evidência da realização do trabalho de campo é mantida até à atribuição da nota em pauta, objeto de eliminação posterior.

- O facto da empresa ao ser parceiro tecnológico na área de consultoria de gestão para inúmeras empresas, torna-a numa ótima escolha;
- Ter a possibilidade, a título gracioso, de contar com serviços de um consultor sénior;
- A estrutura do questionário, os controlos, as ações e as normas de cibersegurança que sustentam o processo;
- Confidencialidade e anonimato.

5.2 DIGNÓSTICO DE MATURIDADE

Breve enquadramento ao *template* do questionário e esclarecimento das possibilidades de resposta ao responsável de TI:

- Sim — 100%;
- Não — 0%;
- Em Progresso — 1% a 99% e a ação está no plano de implementação para os 100% nos próximos 2 anos;
- Inaplicável — a ação não faz parte do âmbito dos processos ou atividades desenvolvidas pela organização.

O entregável consiste na resposta de maturidade da empresa ao nível de segurança e privacidade da informação, via preenchimento do questionário apenso no próprio documento eletrónico da dissertação[2], ou em alternativa através da hiperligação Resposta de Maturidade.

5.3 AVALIAÇÃO DO QUESTIONÁRIO

O questionário, ao ter sido respondido na íntegra, sem auxílio por parte do autor, permite só por si, concluir, estar em estado de maturidade de ser consumido pela audiência a que se destina, ou seja, as PME. No entanto, outros elementos sustentam a afirmação anterior, nomeadamente:

- Disponibilização dos entregáveis, tendo servido de amparo e guia ao respondente, visto indicar o quê e como fazer;

2 Nota do autor: é necessário um visualizador de PDF que suporte anexos embebidos (e.g., *Adobe Acrobat Reader*) para se aceder ao documento.

- Transformação do texto proveniente dos normativos, originalmente apresentado num formato corrido e não esquematizado ou agrupado em ações simplificadas, num conjunto de controlos e subsequentemente, em ações claras e diretas;
- Utilização de *frameworks* com pendor prático.

A Figura 20 mostra o número de respostas por ação, nas opções viáveis.

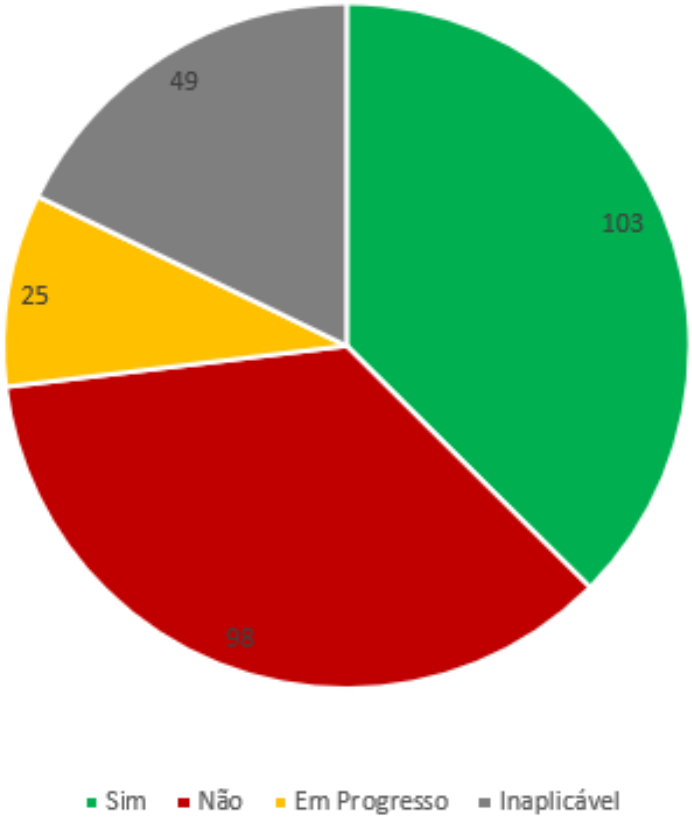


Figura 20: Resultados Agregados por Ação

A primeira apuração é a completude de resposta às 275 ações. A segunda é uma percentagem a rondar os 18%, de respostas da tipologia "Inaplicável". As mesmas concentram-se em seis controlos, resultantes em 39 do total das 49 ações. Tratando-se de uma empresa atuante no setor da consultadoria, as inaplicabilidades têm tendencialmente base de suporte, ora porque não subcontratam serviços tecnológicos e de segurança da informação a terceiros, ora pelos consultores necessitarem de maior liberdade na instalação e parametrização de programas e funcionalidades ao nível do sistema operativo, de modo a prestarem um serviço mais eficaz. No entanto, a metodologia carece de maior aclaração nesta parte. Inaplicabilidade não é sinónimo de exceção ao cumprimento das ações do controlo. Assim, um novo estado da ação é introduzido de nome *Exceção*, significando desvio ao cumprimento da

ação do controlo aprovada pela gestão de topo.

Numa outra perspetiva, a Figura 21 exibe o número de respostas por controlo, em que todas as ações obtiveram a mesma seleção (i.e., "Sim", "Não", "Em Progresso", "Inaplicável"), exceto as colunas "Em Progresso & Não" e "Mescla", esta última aglutina as demais combinações possíveis.

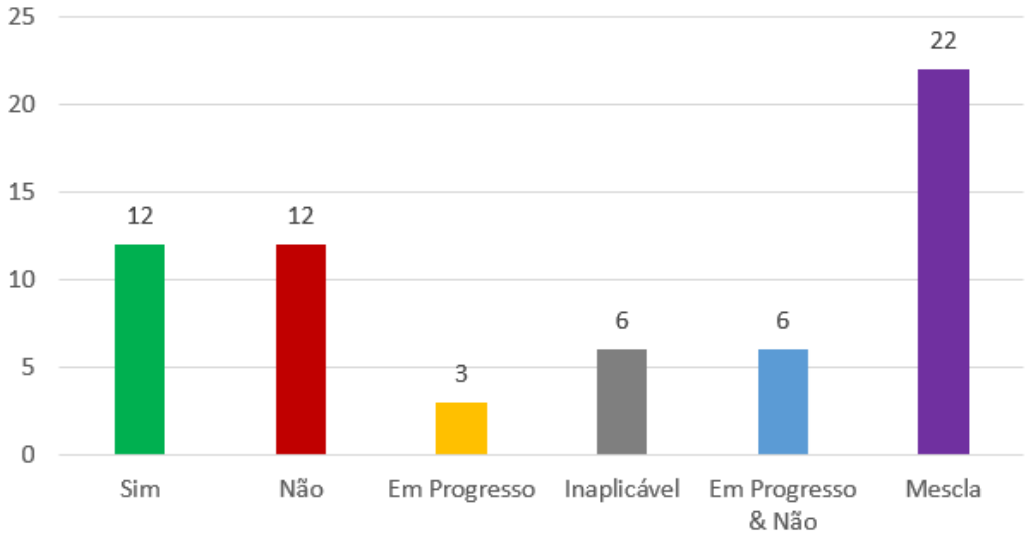


Figura 21: Resultados Agregados por Controlo

Em destaque a predominância de controlos no conjunto "Mescla", aglomerando ações em múltiplos estados, permitindo aferir de modo mais eficiente o grau de completude em cada controlo.

Uma terceira vertente visível nas Figuras 22 e 23, avalia as tipologias e normas de referência, em que todas as ações dos controlos resultaram em "Sim" e "Não".

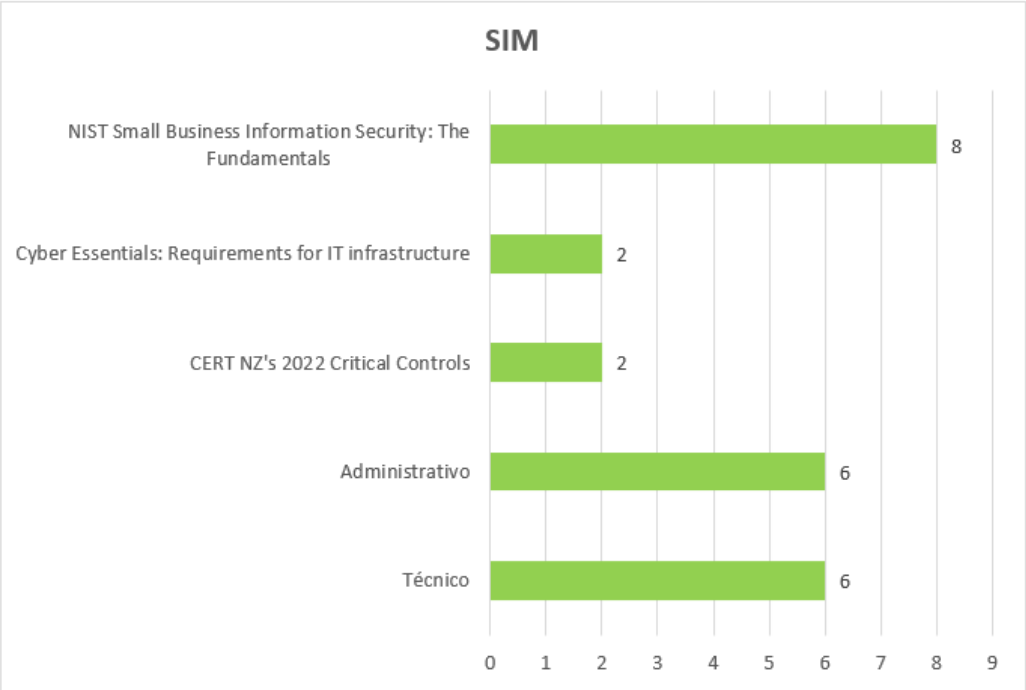


Figura 22: Resultados Agregados por Controlo "Sim"

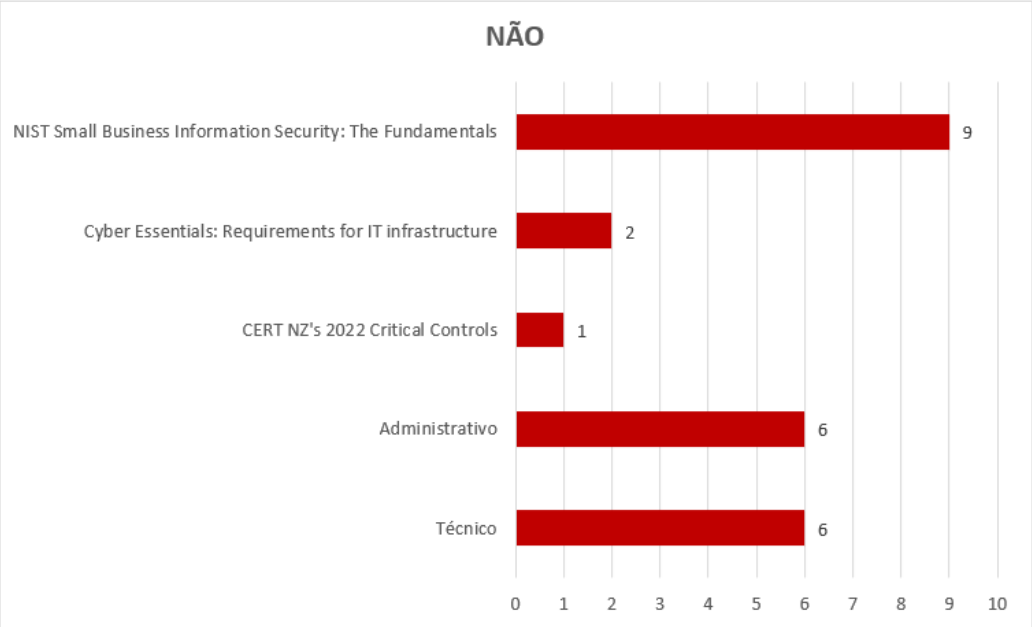


Figura 23: Resultados Agregados por Controlo "Não"

Constata-se ser passível de aferir, desde a primeira iteração de resposta ao questionário, o nível de conformidade por *framework*, conforme se ilustra na Tabela 74.

Tabela 74: Conformidade Normativa Resultante da 1ª Iteração

Framework	**Sim**	**Não**
CERT NZ's 2022 Critical Controls	18.18%	9.09%
Cyber Essencials: Requirements for IT Infrastructure	14.29%	14.29%
NIST Small Business Information Security: The Fundamentals	22.22%	25.00%

É uma estatística importante, caso haja a necessidade por imperativos de negócio, assegurar, numa primeira instância, harmonia face a um normativo singular. Por outro lado, observando as tipologias "Administrativo" e "Técnico", consegue-se tirar deduções, como, por exemplo, se a organização se está a concentrar mais em controlos baseados em políticas ou ferramentas.

Por o modelo de Portfólio de Controlos, apresentado na Tabela 3, estar apetrechado com um rico leque de metadados (e.g., racionalidade, função do controlo, domínios), as ilações que se podem retirar são inúmeras, se não mesmo ilimitadas, dependendo da aguça individual. Dando um exemplo para rematar o anteriormente dito, tendo em conta as respostas de controlos com todas as ações a "Não", fica-se a saber, que em termos dos riscos mencionados no apêndice A, a organização está sujeita a "desvio dos objetivos de negócio", "custo financeiro ou económico" e "exfiltração de dados pessoais", entre outros, pela não aplicação dos controlos.
Em suma, a avaliação da aplicabilidade do questionário, afigura-se claramente positiva pelo já exposto.

5.4 EXPOSIÇÃO DOS RESULTADOS

O processo continua relativamente à empresa, pela apresentação do estado de maturidade da organização, esmiuçando e correlacionando os metadados e indicando o caminho a seguir na defesa dos interesses económicos e estratégicos da organização. Por outro lado, o autor tem particular interesse em captar o modo de como a empresa implementará os entregáveis, na prática, e se os mesmos respondem na íntegra ou se necessitam de ajustes. Também a ordenação de mitigação e os critérios (e.g., riscos, ameaças, tríade CIA) na base de decisão, são dados a serem objeto de estudo.

6

CONCLUSÕES

Colmatar a desarmonia latente entre os saberes da cibersegurança e as estratégias e objetivos de negócio das PME, é o cerne da investigação presente. Dar existência a um SGSPI voltado para o mundo das micros, pequenas e médias empresas nacionais, pela construção de um manual prático munido de ações e entregáveis tangíveis, direciona a presente escrita. Nesta dissertação produziram-se os seguintes elementos:

- 61 controlos elaborados;
- 275 ações derivadas;
- 142 métricas criadas;
- 24 controlos com carácter administrativo e 37 técnicos originados;
- 51 controlos cuja função é de índole preventiva, 3 detetiva e 7 corretiva;
- 49 controlos aglutinam a totalidade da tríade CIA, 5 as propriedades CI, enquanto 3 e 4, respetivamente, ficam-se pelas dimensões C e A;
- 16 domínios agrupam a totalidade dos controlos;
- 22 riscos e 47 ameaças identificadas;
- 24 entregáveis produzidos.

Sucintamente recapitulemos os objetivos[1] definidos e se os mesmos foram conquistados:

1. Construção de um manual prático, em volta das áreas da cibersegurança e proteção de dados munido de entregáveis, que se consiga implementar autonomamente sem recurso a consultores externos;
2. Permitir às PME maior resiliência do seu negócio face aos cibercrimes, aplicando as propostas enunciadas no capítulo 4;
3. Proporcionar aos auditores e gestores de conformidade, a avaliação da completude dos sistemas de gestão de segurança e privacidade onde têm intervenção;

1 Nota do autor: a metodologia não é *per se* um objetivo, mas uma ferramenta auxiliar no processo de produção dos requisitos de cibersegurança.

4. Colocar o foco dos controlos na realidade portuguesa, ou seja, na dimensão socioeconómico das empresas e na legislação nacional e expectativas dos reguladores (e.g., CNPD, CNCS;
5. Possibilitar às empresas uma preparação prévia, para obterem uma certificação de terceira parte em segurança e privacidade da informação, como na ISO/IEC 27701 e por inerência, no RGPD.

O primeiro objetivo foi cumprido no que concerne à produção de controlos e ações diretas, sendo demonstrado no capítulo 5 e na estatística alcançada e esmiuçada no início deste capítulo. Em relação aos entregáveis, é do conhecimento do autor, que os mesmos têm servido de suporte à mitigação das respostas "Não" e em "Em Progresso" e de confirmação dos resultados "Sim" do caso prático. No entanto, é extemporâneo tirar conclusões finais.

O segundo objetivo encontra-se realizado, visto as ações anunciadas no capítulo 4 serem provenientes de normas amplamente práticas e reconhecidas, e a sua implementação, exponenciar sem margem para dúvidas, a ciber-resiliência das organizações. Como exemplo, no caso do recente ataque informático ao Instituto Politécnico de Leiria (IPLEIRIA) (IPL, 2023), se os controlos:

i 1.9.8 — Autenticação Baseada em Múltiplos Fatores;

ii 1.9.16 — Implementar Autenticação Múltiplos Fatores;

iii 1.9.57 — Usar Palavras-passe Fortes;

iv 1.10.39 — Configurar filtros de *web* e *e-mail*;

v 1.19.42 — Formar os Colaboradores.

tivessem sido implementados atempadamente, incluindo as métricas propostas (e.g, "Número de contas de utilizadores regulares com acesso a serviços na nuvem sem um segundo fator de autenticação ativado?"), a probabilidade da ocorrência do ataque de *ransomware* com origem numa mensagem de *phishing* teria sido evitado ou enormemente balizado.

O terceiro objetivo efetuado com sucesso. O autor já usa um conjunto alargado de controlos provenientes do capítulo 4 nas suas atividades profissionais de auditoria à segurança de aplicações digitais. No entanto, a amostra necessita de mais casos de uso de outros profissionais.

O quarto objetivo não se conseguiu atingir, pelos motivos de restrição temporal e de não estender em demasia o capítulo 4 e respetivos apêndices.

O quinto e último objetivo amplamente preenchido no campo da segurança da informação, não tanto no da proteção de dados pessoais.

6.1 CONTRIBUIÇÕES DA INVESTIGAÇÃO

Nesta dissertação foi implementada e testada uma nova metodologia assente nas temáticas da cibersegurança, segurança da informação, privacidade e proteção de dados pessoais: (i) Inquirição de palavras-chave baseadas no âmbito da dissertação; (ii) Seleção de documentação assente em determinados critérios; (iii) Mapeamento de controlos alicerçados em quatro validadores; (iv) Construção do portfólio de controlos e respetivo aperfeiçoamento sustentado em metadados; (v) Roteiro de materialização PME.

Em sintonia com o suprarreferido, infere-se que o mapeamento de normativos com pendor em ações precisas é incompatível. As ações das publicações origem e destino não se mapeiam com a naturalidade expectável. Se o foco estiver no nome do controlo, objetivo, propriedades, tipo, função e domínio, descritos na metodologia, a afinidade é plausível. No entanto, quando se enfatiza as múltiplas ações de cada controlo, não se consegue a tal afinidade, sem diminuir a confiança da percentagem dos valores da Conformidade de Mapeamento (Figura 2) e, consequentemente, produzir um número indesejado de efeitos secundários. Por um lado, a não conformidade com a *framework* em causa, em sede de auditoria de terceira parte. Por outro temos, por excesso ou insuficiência, a aplicação de recursos (e.g., humanos, financeiros, tecnológicos) na realização da ação. No entanto, se o mapeamento se verificar em *frameworks* com pendor em ações qualificáveis e não quantificáveis, baseado em riscos e menos em regras, dando a liberdade de definir a composição dos entregáveis e não no que é expectável se concretizar, então a afinidade torna-se plausível e o mapeamento concretizável.

Adicionalmente é disponibilizado ao tecido empresarial português uma *framework*, resultante da conjugação de múltiplas publicações focadas nas pequenas e médias empresas, recheado de controlos com atividades precisas e respetivos entregáveis, permitindo a implementação de um programa resiliente de cibersegurança, sem recurso a entidades externas e custos desproporcionais subjacente a outras diretrizes. Além disso, os controlos estão enriquecidos com uma panóplia de atributos (e.g., métricas, riscos, ameaças, tipificação), indo além do que é comum se observar neste tipo de publicações, e permitindo às organizações perceberem a real justificação da necessidade de efetivação de cada um dos controlos. A primeira norma escrutinada

assume especial visibilidade, por ser obrigatória a todas as organizações, que queiram realizar certo tipo de contratos governamentais no Reino Unido.

É igualmente introduzida uma abordagem prática à avaliação de risco em seis fases, suportada na identificação, classificação e proteção do ativo. Em remate final, o desenrodilhar dos controlos em ações tangíveis, driblando divagações metafísicas e filosóficas, assessorando as empresas a focar no essencial e relativizar o acessório é, quiçá, o aporte mais expressivo delegado por este estudo.

6.2 RESTRIÇÕES DO ESTUDO

Os 61 controlos produzidos, representam uma fatia basilar significativa de um programa de cibersegurança, mas mantêm a descoberto lacunas, somente mitigadas pela revisão de *frameworks* e legislação adicional. O estudo focou-se nos idiomas português e inglês, descartando, à partida, a integração de outras obras potencialmente relevantes. O trabalho de campo efetuado numa única organização, de natureza e objeto social específico, é uma amostra útil e valiosa, contudo singela. Na metodologia, a radicalização do validador terminal, é sinónimo de uma maior segregação, podendo fluir em determinados falsos positivos. Por outro lado, à medida do aumento exponencial do número de requisitos, a comparação de um novo controlo com os infindáveis restantes, torna-se numa tarefa exigente quando efetuada manualmente.

6.3 TRABALHO FUTURO

Primeiramente o desenlace obtido, serve de esboço à persecução do autor, em conceber um livro prático nas áreas abordadas durante a dissertação, com o foco na proteção física e digital das PME. Em linha com o ponto anterior, o número de *frameworks* a inspecionar e o detalhe das ações e entregáveis será objeto de prosseguimento e exaustiva depuração. Igualmente no encadeamento do já descrito, a utilização de técnicas de aprendizagem automática (e.g., *Cosine Similarity*, *Jaccard Similarity*, *Bilingual Evaluation Understudy*, *Levenshtein Distance*) na comparação de textos em linguagem natural e atribuição de uma pontuação de similaridade, é equacionada como uma preciosa mais-valia, atenuando o esforço despendido na investigação manual através dos quatro validadores, podendo mesmo permitir a substituição do último validador — Conformidade de Mapeamento — em inúmeros casos.

Observando os vários modelos de linguagem natural, *Jaccard Similarity*, apresenta-se como um excelente candidato, pelo facto de medir a paridade entre dois textos, através da comparação de palavras comuns partilhadas entre os excertos origem e destino. O cálculo é efetuado, dividindo o número de palavras comuns, pela total contagem de vocábulos em ambos os textos. O resultado varia entre zero a um, sendo maior a aproximação, quanto mais grandioso o valor for.

Adicionalmente os contributos (e.g., quantificação das respostas - 5.2, novo estado da ação - 5.3, tipificação de alertas a monitorizar - Q) recolhidos durante a implementação do Manual Prático na PME em análise e possíveis comentários a serem recebidos de outras implementações, darão lugar a aperfeiçoamentos.

A realização dos melhoramentos anunciados, têm o intento de dar continuidade ao enriquecimento e consolidação da dissertação, tornando-a numa ferramenta cada vez mais capaz e útil na resposta aos desafios do ciberespaço das PME.

BIBLIOGRAFIA

Abade, Andreia Filipa Constantino (mar. de 2018). «Trabalho de projeto sobre o sistema de controlo interno na área da faturação da empresa Globalwe». Tese de mestrado. Instituto Politécnico de Lisboa - Instituto Superior de Contabilidade e Administração de Lisboa (ISCAL). URL: https://repositorio.ipl.pt/bitstream/10400.21/9362/1/Trabalho%20de%20projeto%20sobre%20o%20SCI%20na%20%C3%A1rea%20da%20Fatura%C3%A7%C3%A3o%20da%20Empresa%20GWE-Andreia%20Abade.pdf.

Alharbi, Fawaz et al. (18 de out. de 2021). «The Impact of Cybersecurity Practices on Cyberattack Damage: The Perspective of Small Enterprises in Saudi Arabia». Em: *Sensors* 21.20, p. 6901. DOI: 10.3390/s21206901.

Alvega, João Manuel Costa (2021). «Privacy awareness in Portuguese SMEs». Tese de mestrado. Universidade de Lisboa, Faculdade de Ciências. URL: http://hdl.handle.net/10451/51906.

Antunes, Mario e Baltazar Rodrigues (2018). *Introdução à Cibersegurança A Internet, os Aspetos Legais e a Análise Digital Forense*. FCA. ISBN: 9789727228614.

Antunes, Mário et al. (8 de abr. de 2021). «Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal». Em: *Journal of Cybersecurity and Privacy* 1.2, pp. 219–238. DOI: 10.3390/jcp1020012.

APWG (set. de 2022). *Phishing Activity Trends Report*. Website. URL: https://docs.apwg.org/reports/apwg_trends_report_q2_2022.pdf.

Ashraf, Saira (mar. de 2021). «GDPR Implementation Framework for SMEs». Tese de mestrado. Metropolia University of Applied Sciences. URL: https://www.theseus.fi/bitstream/handle/10024/493722/Ashraf_Saira.pdf.

Azinheira, Bruno Filipe Diogo (jul. de 2022). «Desenvolvimento de uma metodologia para avaliação do estado da segurança informática em PME». Tese de mestrado. Escola Superior de Tecnologia e Gestão. URL: http://hdl.handle.net/10400.8/7743.

Beborta, Sanket (mai. de 2021). *Preventive, Detective & Corrective Controls*. Website. URL: https://www.linkedin.com/pulse/preventive-detective-corrective-controls-beborta-cisa-crisc-cdpse/.

Bordini, Rubens (1999). *Vida de aviador*. AGE Editora, p. 159. ISBN: 9788585627638.

Brumm, Adam et al. (15 de jan. de 2021). «Oldest cave art found in Sulawesi». Em: *Science Advances* 7.3. DOI: 10.1126/sciadv.abd4648.

BSI (mai. de 2018). *BSI-Standard 200-3: Risk Analysis based on IT-Grundschutz*. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.html.

Cameron, Kim (nov. de 2005). «The Laws of Identity». Em: URL: https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

Carmo Quaresma, Nuno Miguel do (mai. de 2014). «Monitorização de eventos numa PME». Tese de mestrado. Instituto Superior Politécnico Gaya - Escola Superior de Ciência e Tecnologias. URL: http://hdl.handle.net/10400.26/6479.

Cartwright, Mark (set. de 2017). «Paper in Ancient China». Em: *World History Encyclopedia*. URL: https://www.worldhistory.org/article/1120/paper-in-ancient-china/.

Carvalho Silva, Gustavo de (fev. de 2020). «RGPD aplicado nas PME portuguesas». Tese de mestrado. Universidade Nova de Lisboa - Instituto Superior de Estatística e Gestão de Informação. URL: http://hdl.handle.net/10362/94888.

Cavins, Jeff (jun. de 2022). *The Art of Learning and Deep Fat Fridays*. Website. URL: https://media.ascensionpress.com/podcast/the-art-of-learning-and-deep-fat-fridays/.

Cempalavras (fev. de 2022). *Guia de Empresas Certificadas 2021-2022*. URL: https://issuu.com/cempalavras.pt/docs/gec_2021_pt.

Center, Vanderbilt University Medical (s.d.). *Are there Different Types of Internal Controls?* URL: https://www.vumc.org/vumcinternalaudit/are-there-different-types-internal-controls.

Chak, Stephanie K. (mai. de 2015). «Managing cybersecurity as a business risk for small and medium enterprises». Tese de mestrado. Johns Hopkins University. URL: https://jscholarship.library.jhu.edu/bitstream/handle/1774.2/38027/CHAK-THESIS-2015.pdf.

Chamberlain, Aaron (dez. de 2021). «Beginning the information security journey for small and medium enterprises through business continuity planning and infrastructure automation». Tese de mestrado. California State University, San Bernardino. URL: https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=2521&context=etd.

Channnel, IT (jan. de 2022). *Ciberataques a organizações portuguesas aumentaram 81% em 2021*. Website. URL: https://www.itchannel.pt/news/seguranca/ciberataques-a-organizacoes-portuguesas-aumentaram-81-em-2021.

Cichonski, Paul et al. (ago. de 2012). *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology*. DOI: 10.6028/nist.sp.800-61r2.

CISA (nov. de 2021). *Federal Government Cybersecurity Incident & Vulnerability Response Playbooks*. URL: https://www.cisa.gov/sites/default/files/2023-02/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.

CMMI Product Team (2010). «CMMI for Development, Version 1.3». Em: DOI: 10.1184/R1/6572342.V1.

CNCS (jun. de 2022). *Cibersegurança em Portugal - Riscos & Conflitos*. Rel. téc. URL: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf.

Commission, European, Entrepreneurship Directorate-General for Internal Market Industry e SMEs (2020). *User guide to the SME definition*. Publications Office. DOI: doi/10.2873/255862.

Cook, Kimberly Diane (2017). «Effective Cyber Security Strategies for SmallBusinesses». Tese de doutoramento. Walden University. URL: https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=4974&context=dissertations.

Curtis, Blake (jul. de 2020). *What Is the Difference Between Requirements and Controls?* Website. URL: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/what-is-the-difference-between-requirements-and-controls.

Deloitte (2022). *Dados: o ativo de maior valor*. Website. URL: https://www2.deloitte.com/pt/pt/hot-topics/dados-o-ativo-de-maior-valor.html.

Demo, Pedro (1995). *Metodologia Científica em Ciências Sociais*. Ed. por Atlas S.A. 3ª ed. ISBN: 8522412413.

Dempsey, K L et al. (2011). *Information Security Continuous Monitoring (ISCM) for federal information systems and organizations*. Rel. téc. DOI: 10.6028/nist.sp.800-137.

Diligent (fev. de 2022). *Relationships between controls and requirements*. Website. URL: https://help.highbond.com/helpdocs/controlsbond/en-us/Content/projects/compliance/relationships_between_controls_and_requirements.htm.

DN (set. de 2022). *Hackers publicam dados de 1,5 milhões de clientes da TAP*. Website. URL: https://www.dn.pt/sociedade/hackers-publicam-dados-de-15-milhoes-de-clientes-da-tap-15179930.html.

DOMO (2022). *Data Never Sleeps 9.0*. Website. URL: https://web-assets.domo.com/blog/wp-content/uploads/2021/09/data-never-sleeps-9.0-1200px-1.png.

Eramba (s.d.). *Welcome to OpenSourceGRC FAQ*. Website. URL: https://docs.google.com/document/d/1ov4V1Ou7r69KOqXjxlK5R77jrgc-JOEhzFe545_pqaU/edit#.

Espinosa, Christian (set. de 2021). *Top 10 Organized Cybercrime Syndicates*. Website. URL: https://christianespinosa.com/blog/top-10-organized-cybercrime-syndicates/.

EUR-Lex (abr. de 2016). *REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

European Union, Publications Office of the (mai. de 2003). «COMMISSION RECOMMENDATION of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises». Em: *Official Journal of the European Union* 46.L 124, pp. 36–38. ISSN: 1725-25555. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2003:124:FULL&from=EN.

Faria, Cláudia Maria Félix Leite de (2018). «Gestão da Cibersegurança em empresas Transnacionais relacionadas com Transações Financeiras Críticas de espectro Macroeconómico». Tese de mestrado. Departamento de Ciência de Computadores - Universidade do Porto. URL: https://repositorio-aberto.up.pt/bitstream/10216/118687/3/312224.1.pdf.

Ferraiolo, Hildegard et al. (jul. de 2015). *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*. Rel. téc. DOI: http://dx.doi.org/10.6028/NIST.SP.800-79-2.

Ferreira, Haroldo (dez. de 2021). *Cibersegurança*. Ed. por Senac.

Fischer, German (2020). «Guidelines for SME adaption to GDPR Case study of Evalent». Tese de mestrado. Luleå University of Technology - Department of Computer Science, Electrical e Space Engineering. URL: https://www.diva-portal.org/smash/get/diva2:1442458/FULLTEXT01.pdf.

Force, Joint Task (set. de 2020). *Security and Privacy Controls for Information Systems and Organizations*. Rel. téc. DOI: 10.6028/nist.sp.800-53r5.

Gallistel, Charles Randy (ago. de 2015). *Bayes for Beginners: Probability and Likelihood*. Website. URL: https://www.psychologicalscience.org/observer/bayes-for-beginners-probability-and-likelihood.

Garcia, Cátia Marisa Rodrigues (out. de 2017). «Implementação de um Sistema de Controlo Interno numa Entidade do Setor Não Lucrativo». Tese de mestrado. Instituto Politécnico de Tomar. URL: https://comum.rcaap.pt/bitstream/10400.26/21302/1/Implementa%C3%A7%C3%A3o%20de%20um%20SCI%20numa%20ESNL_C%C3%A1tia%20Garcia_Revisto.pdf.

Garfinkel, Simson L. (out. de 2015). *De-identification of personal information*. Rel. téc. DOI: 10.6028/nist.ir.8053.

Hughes, J. Trevor e Kabir Barday (mar. de 2018). «IAPP-OneTrust Research: Bridging ISO 27001 to GDPR». Em: p. 12. URL: https://iapp.org/media/pdf/resource_center/IAPP-OneTrust-Bridging-ISO-GDPR-final.pdf.

IPL (mai. de 2023). *Ciberataque às Infraestruturas de Comunicação e de Informação do Politécnico de Leiria*. URL: https://www.ipleiria.pt/informacao-ciberataque-as-infraestruturas-de-comunicacao-e-de-informacao-do-politecnico-de-leiria/.

IRI (s.d.). *A Compliance Toolkit for GDPR*. URL: https://www.iri.com/ftp9/pdf/FieldShield/IRI_GDPR_Compliance_Toolkit.pdf.

Isabel Martins, Georgina Morais e (2013). *Auditoria Interna*. 4ª. Áreas Editora. ISBN: 9789898058812.

Jideani, Paul Chimdbiebere (nov. de 2018). «Towards a cybersecurity framework for South African e-retail organizations». Tese de mestrado. Cape Peninsula University of Technology - Faculty of Informatics e Design. URL: https://etd.cput.ac.za/bitstream/20.500.11838/2958/1/jideani_paul_209089067.pdf.

Johnson, Steve (set. de 2022). *Security, risk and compliance: An alternative approach*. Website. URL: https://cyberstartupobservatory.com/security-risk-and-compliance-an-alternative-approach/.

JTC1/SC27 (out. de 2005). *ISO/IEC 27001:2005 - Information technology — Security techniques — Information security management systems — Requirements*.

— (fev. de 2018a). *ISO/IEC 27000:2018 - Information technology — Security techniques — Information security management systems — Overview and vocabulary*.

— (jul. de 2018b). *ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management*.

— (out. de 2019). *ISO/IEC 27701:2019 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*.

JTC1/SC27 (out. de 2022a). *ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.

— (fev. de 2022b). *ISO/IEC 27002:2022 - Information security, cybersecurityand privacy protection — Informationsecurity controls*.

Lechêne, Robert (1 de out. de 2020). «Printing». Em: *Encyclopedia Britannica*. URL: https://www.britannica.com/topic/printing-publishing/History-of-printing.

LookingGlass (s.d.). *Three Common Threat Actors and the One You Might Not Know About*. URL: https://lookingglasscyber.com/blog/threat-intelligence-insights/three-common-threat-actors-and-the-one-you-might-not-know-about/.

Lopes, Ana Cristina M. e Graça Maria Rio-Torto (2007). *Semântica*. Ed. por Caminho. Vol. Volume 6 of Colecção o essencial sobre língua portuguesa. Caminho, p. 98. ISBN: 9789722118781.

Louisville, University of (s.d.). *Internal Controls*. Website. URL: https://louisville.edu/audit/internal-controls.

Lusa/DN (set. de 2022). *EUA propõem colaboração com Portugal após ciberataque que expôs dados da NATO*. Website. URL: https://www.dn.pt/sociedade/eua-propoem-colaboracao-com-portugal-apos-ciberataque-que-expos-dados-da-nato-15170011.html.

Marshall, Catherine, Gretchen B. Rossman e Gerardo L. Blanco (mai. de 2021). *Designing qualitative research*. Ed. por SAGE Publishing. 7th. SAGE. ISBN: 9781071817360.

Matos, Pedro Carvalhais de Abreu (dez. de 2018). «Cibersegurança: políticas públicas para uma cultura de cibersegurança nas empresas». Tese de mestrado. Iscte - Instituto Universitário de Lisboa. URL: http://hdl.handle.net/10071/17630.

McKinsey (jan. de 2022). *The data-driven enterprise of 2025*. Website. URL: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-data-driven-enterprise-of-2025.

Monteiro, Ana Maria Dias (2015). «A Avaliação do Sistema de Controlo Interno: o contributo do auditor externo e o seu papel na gestão empresarial». Tese de mestrado. Faculdade de Economia do Porto. URL: https://repositorio-aberto.up.pt/bitstream/10216/80559/2/36588.pdf.

Morris, R e B Truskowski (2003). «The evolution of storage systems». Em: *IBM Systems Journal* 42.2, pp. 205–217. DOI: 10.1147/sj.422.0205.

Morse, Alan e Char McEvoy (out. de 2014). «Qualitative Research in Sport Management: Case Study as a Methodological Approach». Em: *The Qualitative Report*. DOI: https://doi.org/10.46743/2160-3715/2014.1032.

Nabila, Amrin (2014). «The Impact of Cyber Security on SMEs». Tese de mestrado. University of Twente - Faculty of Electrical Engineering, Mathematics e Computer Science.

NCSC (jan. de 2022). *Cyber Essentials: Requirements for IT infrastructure*. Rel. téc. V3.0. National Cyber Security Centre. URL: https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-0-January-2022.pdf.

Negócios, Jornal de (jul. de 2022). *Portugal sofreu 3 mil ataques informáticos nos primeiros três meses do ano*. Website. URL: https://www.jornaldenegocios.pt/empresas/tecnologias/detalhe/portugal-sofreu-3-mil-ataques-informaticos-nos-primeiros-tres-meses-do-ano.

NZ, CERT (fev. de 2022). *CERT NZ's Critical Controls 2022*. Website. URL: https://www.cert.govt.nz/assets/Uploads/documents/cert-nz-2022-critical-controls.pdf.

Oberländer Anna Maria; Lösser, Benedict; e Daniel Rau (jun. de 2019). «Taxonomy research in information systems: a systematic assessment». Em: URL: https://aisel.aisnet.org/ecis2019_rp/144.

Offers, Julius (jun. de 2020). «Understanding factors influencing SME's decision makers when implementing cybersecurity measures: a protection motivation perspective». Tese de mestrado. Leiden University - Faculty of Governance e Global Affairs. URL: https://studenttheses.universiteitleiden.nl/access/item:3190969/view.

Oliveira, Ricardo João Duque (mai. de 2014). «A importância dos controlos técnicos preventivos e detetivos nas redes de dados da Administração Pública». Tese de mestrado. Universidade Católica Portuguesa - Faculdade de Engenharia. URL: https://repositorio.ucp.pt/bitstream/10400.14/15012/1/Tese_RJDO_v1.1.pdf.

OWASP (dez. de 2020). *OWASP Web Security Testing Guide - Testing for Weak Encryption*. Website. URL: https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/09-Testing_for_Weak_Cryptography/04-Testing_for_Weak_Encryption.html.

Parker, Donn B. (1998). *Fighting computer crime. a new framework for protecting information*. Wiley, p. 512. ISBN: 978-0471163787.

Patton, Michael Quinn (jan. de 2015). *Qualitative Research and Evaluation Methods Integrating Theory and Practice. Integrating Theory and Practice*. Ed. por SAGE Publishing. 4th. SAGE Publications, Limited, p. 832. ISBN: 9781412972123.

Paulsen, Celia e Patricia Toth (out. de 2016). *Small Business Information Security: The Fundamentals*. Rel. téc. DOI: https://doi.org/10.6028/NIST.IR.7621r1.

PCI (nov. de 2012). *Information Supplement: PCI DSS Risk Assessment Guidelines*. URL: https://listings.pcisecuritystandards.org/documents/PCI_DSS_Risk_Assmt_Guidelines_v1.pdf.

Pesce, Lucila (mar. de 2009). *Características da investigação qualitativa*. Website. URL: https://www.slideshare.net/lucilapesce/caractersticas-da-investigao-qualitativa.

Pinto, Isabel Ferraz, Claudinei José Gomes Campos e Cibele Siqueira (set. de 2018). «Investigação qualitativa: perspetiva geral e importância para as ciências da nutrição». Em: *Acta Portuguesa de Nutrição*. URL: https://actaportuguesadenutricao.pt/wp-content/uploads/2018/11/06_Investiga%C3%A7%C3%A3o-qualitativa-Perspetiva-geral-e-import%C3%A2ncia-para-as-Ci%C3%AAncias-da-Nutri%C3%A7%C3%A3o.pdf.

Pordata (s.d.). *Pequenas e Médias Empresas (PME)*. Website. URL: https://www.pordata.pt/Subtema/Portugal/Pequenas+e+M%C3%A9dias+Empresas+(PME)-378.

ProtonTechnologies (s.d.). *GDPR compliance checklist - GDPR.eu*. URL: https://gdpr.eu/checklist/.

Reciprocity (jan. de 2022). *What are the 3 Types of Internal Controls?* Website. URL: https://reciprocity.com/resources/what-are-the-3-types-of-internal-controls/.

Rifkin, Jeremy (2011). *The third industrial revolution how lateral power is inspiring a generation and transforming the world. How Lateral Power Is Transforming Energy, the Economy, and the World*. Palgrave Macmillan, p. 304. ISBN: 978-0230115217.

Ruefle, Robin (jan. de 2007). *Defining Computer Security Incident Response Teams*. Software Engineering Institute, Carnegie Mellon University. 4500 Fifth Avenue-Pittsburgh, PA 15213-2612. URL: https://resources.sei.cmu.edu/asset_files/WhitePaper/2007_019_001_294579.pdf.

Saber, Jennifer (2016). «Determining Small Business Cybersecurity Strategies to Prevent Data Breaches». Tese de doutoramento. Walden University. URL: https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=6270&context=dissertations.

SAPO (jul. de 2022). *Impresa perde 2,2 milhões no semestre do ciberataque. Horta Osório será vice-presidente*. Website. URL: https://eco.sapo.pt/2022/07/28/impresa-tem-prejuizo-de-22-milhoes-no-semestre-do-ciberataque/.

Savkin, Aleksey (2017). *10 Step Kpi System*. Lulu Press, Inc. ISBN: 9781365900716.

Silva, Michel Bernardo Fernandes da (jan. de 2023). *Cibersegurança: Visão Panorâmica Sobre a Segurança da Informação na Internet*. Freitas Bastos. 288 pp. ISBN: 9786556752457. URL: https://www.ebook.de/de/product/45505773/michel_bernardo_fernandes_da_silva_ciberseguranca.html.

Silva Baptista, Isabel Margarida Afonso da (out. de 2017). «O fator humano na cibersegurança». Tese de mestrado. Instituto Superior Técnico. URL: https://fenix.tecnico.ulisboa.pt/downloadFile/1407770020546276/Dissertacao_IMB_vF.pdf.

Stanfield, Nathan (dez. de 2019). *11 Firewall Features You Can't Live Without*. Website. URL: https://www.stanfieldit.com/11-firewall-features/.

SunnyValleyNetworks (s.d.). *What are the Top Must-Have Features of a Next-Generation Firewall?* URL: https://www.sunnyvalley.io/docs/network-security-tutorials/what-are-the-top-must-have-features-of-a-next-generation-firewall.

Taherdoost, Hamed (jul. de 2022). «Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview». Em: *Electronics* 11.14, p. 2181. DOI: https://doi.org/10.3390/electronics11142181. URL: https://www.mdpi.com/2079-9292/11/14/2181/htm.

TeachComputerScience (s.d.). *Firewall*. URL: https://teachcomputerscience.com/firewall/.

Tipton, Harold F. e Micki Krause (2007). *Information Security Management Handbook, Sixth Edition (Isc2 Press)*. AUERBACH, p. 3231. ISBN: 9780849374951.

Tzu, Sun (abr. de 2020). *Art of War*. Diamond Books. 104 pp. ISBN: 9789390960033. URL: https://www.ebook.de/de/product/41757234/sun_tzu_art_of_war.html.

Walkowski, Debbie (ago. de 2019). *What Are Security Controls?* Website. URL: https://www.f5.com/labs/learning-center/what-are-security-controls.

Whitehead, Gerard (ago. de 2020). «Investigation of factors influencing cybersecurity decision making in Irish SME's from a senior manager/owner perspective». Tese de mestrado. National College of Ireland - School of Business. URL: https://norma.ncirl.ie/4804/1/gerardwhitehead.pdf.

Young, Dr. Bill (s.d.). *Foundations of Computer Security - Lecture 4: Aspects of Security*. Website. URL: https://www.cs.utexas.edu/~byoung/cs361/lecture4.pdf.

Zec, Milos (jun. de 2015). «Cyber security Measures in SMEs: a study of IT professionals' organizational cyber security awareness». Tese de mestrado. Linnaeus University - Department of Technology. URL: https://www.diva-portal.org/smash/get/diva2:849211/ATTACHMENT01.pdf.

APÊNDICES

APÊNDICE A — RISCOS NA AUSÊNCIA DE CONTROLOS

Tabela 75: Riscos na Ausência de Controlos

#	**Risco**
1	Afastamento estratégico
2	Alienação em investimento tecnológico e inovação
3	Cobertura negativa dos meios de comunicação social
4	Coima
5	Custo financeiro ou económico
6	Dano reputacional ou perda de credibilidade
7	Desinvestimento em capacitação humana
8	Desvio dos objetivos de negócio
9	Disrupção da cadeia de fornecimento
10	Exfiltração de dados pessoais
11	Expectativas logradas por parte dos clientes em relação a produtos e/ou ou serviços oferecidos
12	Impacto negativo em interesses económicos e comerciais
13	Incapacitação de ativos corporativos
14	Incumprimento de contrato ou acordo com partes interessadas
15	Infração legislativa, regulatória ou regulamentar
16	Insegurança das pessoas
17	Perda de competitividade
18	Quebra de segurança e privacidade de dados
19	Rutura de atividades ou operações
20	Tempo despendido pela gestão de topo na contenção e resolução da crise ou incidente
21	Vazamento de dados de negócio
22	Violação de políticas e de outras conformidades corporativas

B

APÊNDICE B — RESUMO DAS AMEAÇAS ELEMENTARES

Tabela 76: Resumo das Ameaças Elementares

#	**Ameaça**	**Propriedades afetadas diretamente pela Ameaça**
1	Acesso não autorizado a sistemas TI	C,I
2	Água	I,A
3	Ataque	C,I,A
4	Avarias de dispositivos ou sistemas	C,I,A
5	Catástrofes naturais	A
6	Catástrofes no meio ambiente	A
7	Coerção, extorção ou corrupção	C,I,A
8	Condições ambientais desfavoráveis	I,A
9	Destruição de dispositivos ou suporte de dados	A
10	Divulgação de informação que devia estar protegida	C
11	Efeitos secundários prejudiciais	C,I,A
12	Engenharia social	C,I
13	Entrada não autorizada em compartimentos	C,I,A
14	Espionagem	C
15	Falha de dispositivos ou sistemas	A
16	Falha ou mau funcionamento das rede de fornecimento	A
17	Falha ou mau funcionamento das redes de comunicação	I,A
18	Falha ou mau funcionamento dos prestadores de serviço	C,I,A
19	Falta de Recursos	A
20	Fogo	A
21	Fontes de dados não fidedignas	C,I,A
22	Importação de mensagens	C,I
23	Interceção de comunicações	C
24	Intercepção de radiação comprometedora	C
25	Interferência eletromagnética	I,A
26	*Malware*	C,I,A
27	Manipulação de *hardware* ou *software*	C,I,A
28	Manipulação de informação	I
29	Negação de serviços	A
30	Perda de dados	A
31	Perda de dispositivos, suportes de dados e documentos	C,A
32	Perda de integridade da informação que devia estar protegida	I
33	Perda de pessoas	A
34	Perturbação ou mau funcionamento do fornecimento de energia	I,A
35	Planeamento deficiente ou falta de ajustamento	C,I,A
36	Principais eventos no meio ambiente	C,I,A
37	Repúdio de atos	C,I
38	Roubo ou furto de dispositivos, suportes de dados e documentos	C,A
39	Sabotagem	A
40	Sujidade, pó, corrosão	I,A
41	Usurpação de identidade	C,I,A
42	Utilização indevida de autorizações	C,I,A
43	Utilização indevida de dados pessoais	C
44	Utilização ou administração incorreta de dispositivos e sistemas	C,I,A
45	Utilização ou administração não autorizada de dispositivos e sistemas	C,I,A
46	Violação de leis ou contratos	C,I,A
47	Vulnerabilidades ou erros de *software*	C,I,A

C

APÊNDICE C — MATRIZ DE MAPEAMENTO

Tabela 77: Matriz de Mapeamento

#	Nome do Controlo	GB	NZ	US
1	Âmbito de Aplicabilidade	X		
2	Proteção de Perímetro	X		
3	*Software Firewall*	X		
4	Robustez da Configuração Inicial do Sistema	X		
5	Desbloqueio Seguro do Sistema	X		
6	Ciclo de Vida das Contas dos Utilizadores	X		
7	Autenticação Baseada em Segredos	X		
8	Autenticação Baseada em Múltiplos Fatores	X		
9	Proteção de Código Malicioso	X		
10	Aplicações Autorizadas	X		
11	Isolamento e Segregação Aplicacional	X		
12	Gestão das Atualizações de Segurança	X		
13	Gestão do Licenciamento de *Software*	X		
14	Salvaguarda dos Dados	X		
15	Atualização do *Software* e Sistemas		X	
16	Implementar Autenticação Múltiplos Fatores		X	
17	Providenciar e Utilizar um Gestor de Segredos		X	
18	Configuração de Registos e Alertas		X	
19	Ciclo de Vida dos Ativos		X	
20	Implementar e Testar as Salvaguardas		X	
21	Implementar Controlo Aplicacional		X	
22	Aplicar o Princípio do Menor Privilégio		X	
23	Implementar Segmentação de Rede		X	
24	Definir Padrões Seguros para Macros		X	
25	Implementar Processo de Negócio de Verificação		X	
26	Identificar a Informação Armazenada e Utilizada			X
27	Determinar o valor da informação			X
28	Elaborar um Inventário de Informação			X
29	Compreender as Ameaças e Vulnerabilidades do Negócio			X
30	Identificar e Controlar quem tem acesso à Informação de Negócio			X
31	Realizar Verificação de Antecedentes			X
32	Exigir Contas de Utilizador Individuais para Cada Colaborador			X
33	Criar Políticas e Procedimentos de Segurança da Informação			X
34	Limitar o Acesso do Colaborador a Dados e Informação			X
35	Instalar Supressores de Pico de Tensão e Fontes de Alimentação Ininterrupta			X
36	Atualização de Sistemas Operativos e Aplicações			X
37	Instalar e Ativar *Firewalls* de *Software* e *Hardware* em todas as Redes Corporativas			X
38	Proteger os Pontos de Acesso sem Fios e as Redes			X
39	Configurar filtros de *Web* e *E-mail*			X
40	Usar Criptografia para Informações Confidenciais de Negócio			X
41	Eliminação Segura de Computadores Obsoletos e Suportes de Armazenamento			X
42	Formar os Colaboradores			X
43	Instalar e Atualizar Programas de Antivírus, *Spyware* e Outros *Anti-malware*			X
44	Manter e Monitorizar os Registos			X
45	Desenvolver um Plano para Desastres e Incidentes de Segurança da Informação			X
46	Concretizar Cópias de Segurança Completas de Dados / Informações de Negócio Importantes			X
47	Efetuar Cópias de Segurança Incrementais de Dados / Informações de Negócio Importantes			X
48	Considerar um Seguro de Cibersegurança			X
49	Realizar Melhorias a Processos / Procedimentos / Tecnologias			X
50	Prestar Atenção às Pessoas do Trabalha e em Redor			X
51	Ter Cuidado com os Anexos de *E-mail* e as ligações *Web*			X
52	Utilizar Computadores, Dispositivos Móveis e Contas Pessoais e Corporativas Separadas			X
53	Não Conectar Dispositivos Pessoais ou de Armazenamento não Confiáveis, ou *Hardware* no Computador, Dispositivo Móvel, ou Rede Corporativa			X
54	Tomar Precauções na Transferência de *Software*			X
55	Não Fornecer informações Pessoais ou de Negócio			X
56	Estar Atento aos *Pop-ups* Nocivos			X
57	Usar Palavras-passe Fortes			X
58	Conduzir Negócios *On-line* de Modo mais Seguro			X
59	Subcontratar Serviços Tecnológicos e de Segurança da Informação			X
60	Executar Varredura de Vulnerabilidades			X
61	Conduzir Teste de Intrusão			X

Legenda: GB - GB.NCSC.CE | NZ - NZ.CERT.NZ.CC | US - US.NIST.SBIS.TF

C.0.1 *Processo de Validação Exaustivo*

Observando todos as *frameworks*[1] numa única tabela (10, 25, 37) e filtrando pelo primeiro validador — a tríade CIA — verificamos a existência de quatro hipóteses: (i) A; (ii) C; (iii) CI; (iv) CIA.

- Propriedade A: depurando os resultados pelo atributo Disponibilidade, vislumbram-se quatros controlos (i.e., 24, 31, 58, 59), amparados pelo domínio treze, a função "Corretivo" e a tipologia "Técnica". Além disso, esquadrinhando o nome de cada controlo — "Salvaguarda dos Dados", "Implementar e Testar as Salvaguardas", "Concretizar Cópias de Segurança Completas de Dados / Informações de Negócio Importantes", "Efetuar Cópias de Segurança Incrementais de Dados / Informações de Negócio Importantes" — existem relações de equivalência semântica. Avançando para o derradeiro validador, não se aferem quaisquer conformidades de mapeamento "preciso" ou "suficiente", sendo, portanto, objeto de descarte.

Identificador	Nome	Item	Ações	14 p/ 20	14 p/ 46	14 p/ 47
1.13.14	Salvaguarda dos Dados	1	Salvaguardar a informação regularmente.	2	0	0
		2	Copiar a informação salvaguardada num outro repositório local ou remoto.	0	0	0
		3	Habilitar salvaguardas automáticas, sempre que possível.	2	0	0
		4	Salvaguardas efetuadas para discos externos *usb* devem ser desconectados após a realização da tarefa.	0	0	0

Figura 24: Conformidade de Mapeamento do Controlo 1.13.14

Identificador	Nome	Item	Ações	20 p/ 14	20 p/ 46	20 p/ 47
1.13.20	Implementar e Testar as Salvaguardas	1	O responsável por cada conjunto de dados toma decisões em torno da importância e dos tempos de recuperação dos mesmos (objetivos de recuperação). A equipa deTI fornece aconselhamento sobre os objetivos de recuperação.	0	0	0
		2	As cópias de segurança são realizadas automática e regularmente. O calendário é baseado nos objetivos de recuperação da organização.	1 3	0	0
		3	Enviar alertas para quaisquer falhas de cópias à equipa responsável pelas salvaguardas e aos donos dos dados.	0	0	0
		4	Testar regularmente as cópias de segurança usando diferentes casos de uso. Por exemplo, testar a reposição de um único ficheiro, pelo menos uma vez por trimestre, e testar uma recuperação completa, pelo menos uma vez por ano.	0	6	6

Figura 25: Conformidade de Mapeamento do Controlo 1.13.20

1 Nota do Autor: a carência de conformidade do mapeamento das normas supracitadas, pode levar o leitor a cogitar, da inexistência de compatibilidade entre toda e qualquer publicação e a metodologia empregue, não sendo de todo o caso. Tomando como amostra a ISO/IEC 27001:2022 (JTC1/SC27, 2022a), é de trivial argumentação a presença de pontos de união. Por exemplo, o controlo 5.9 *Inventory of information and other associated assets — An inventory of information and other associated assets, including owners, shall be developed and maintained*, tem uma simetria com o controlo 1.6.28 (Tabela 40) — Elaborar um Inventário de Informação.

Identificador	Nome	Item	Ações	5.9 p/ 28
5.9	*Inventory of information and other associated assets*	1	*An inventory of information and other associated assets, including owners, shall*	1 a 7

Identificador	Nome	Item	Ações	28 p/ 5.9
1.6.28	Elaborar um Inventário de Informação	1	Identificar a tecnologia, i.e., *hardware* e *software*, usada para armazenar, aceder, processar e transmitir os diversos tipos de informação.	1
		2	Incluir a marca, modelo, números de série, e outras informações de	1
		3	Todos os tipos de informação devem ter, pelo menos, uma tecnologia de *hardware* / *software* listada. Quando aplicável, incluir tecnologias fora do negócio (por exemplo, "a nuvem") e quaisquer tecnologias de proteção	1
		4	Rastrear a localização de cada tipo de informação.	1
		5	Associar o dono da tecnologia, se aplicável.	1
		6	Determinar o impacto global potencial da informação.	1
		7	Atualizar o inventário, pelo menos anualmente.	1

Identificador	Nome	Item	Ações	47 p/ 46	47 p/ 20	47 p/ 14
1.13.46	Concretizar Cópias de Segurança Completas de Dados / Informações de Negócio Importantes	1	Realizar uma cópia de segurança completa e encriptada dos dados em cada computador e dispositivo móvel utilizado no negócio, pelo menos uma vez por mês, pouco depois de uma varredura completa do antivírus.	0	0	0
		2	Armazenar as cópias de segurança, numa localização diferente da do edifício, onde se realizam as salvaguardas.	0	0	0
		3	Guardar uma cópia da senha ou chave de encriptação, num local seguro e separado do local onde se encontram as cópias de segurança armazenadas.	4	0	0
		4	Encriptar todos os dados, antes de salvaguardar as cópias num prestador de serviços na nuvem.	0	0	0
		5	Reter as cópias de segurança por um ano.	5	0	0
		6	Testar as cópias de segurança, imediatamente após a sua criação.	0	4	0

Figura 26: Conformidade de Mapeamento do Controlo 1.13.46

Identificador	Nome	Item	Ações	46 p/ 47	46 p/ 20	46 p/ 14
1.13.47	Efetuar Cópias de Segurança Incrementais de Dados / Informações de Negócio Importantes	1	Conduzir um *backup* automático incremental ou diferencial de cada um dos computadores e dispositivos móveis corporativos, pelo menos uma vez por semana.	0	0	0
		2	Armazenar as cópias de segurança, em suporte amovível, num servidor isolado da rede, ou na nuvem.	0	0	2
		3	Encriptar os *backups*.	0	0	0
		4	Guardar uma cópia da senha ou chave de encriptação, num local seguro e separado do local onde se encontram as cópias de segurança armazenadas.	3	0	0
		5	Reter as cópias de segurança por 52 semanas.	5	0	0
		6	Testar as cópias de segurança periodicamente.	0	4	0

Figura 27: Conformidade de Mapeamento do Controlo 1.13.47

- Propriedade C: filtrando pela Confidencialidade surgem três controlos (i.e., 28, 53, 67) pertencentes a três domínios (ver Tabela 5) diferentes, nove, quinze e dezanove respetivamente. A falha do domínio interrompe o processo de validação e descarta o mapeamento.
- Propriedade CI: selecionado os parâmetros Confidencialidade e Integridade aparecem cinco controlos 14, 15, 35, 36 e 52 sustentados em três domínios. Somente os três primeiros controlos comungam da mesma família, de nome, "Gestão das Configurações". Também têm a mesma função "Preventivo" e são do tipo "Técnico". Esmiuçando o valor semântico do nome dos controlos — "Robustez da Configuração Inicial do Sistema", "Desbloqueio Seguro do Sistema" e "Definir Padrões Seguros para Macros" — verificam-se relações de não equivalência sinonímia entre outras. Portanto, os controlos são descartados no processo de mapeamento.
- Propriedade CIA: escrutinando os quarenta e novo controlos resultantes e aplicando o mesmo método, descrito anteriormente para os três primeiros validadores, existem vinte possibilidades de conformidade de mapeamento. Os quadros adjacentes descortinam a carência de qualquer relação "Preciso" ou "Suficiente", sendo novamente desígnio de enjeitamento.

Identificador	Nome	Item	Ações	18 p/ 44
1.2.18	Configuração de Registos e Alertas	1	Habilitar o registo para eventos críticos para o negócio ou que envolvem dados sensíveis.	0
		2	Sincronizar todos os sistemas à mesma fonte temporal e a um fuso horário consistente, para facilitar a análise e correlação.	0
		3	Enviar os registos para um sistema de armazenamento e análise centralizado.	0
		4	O sistema central de agregação de registos deve ter um acesso limitado, somente de leitura, aos utilizadores que dele necessitam. Alterações e eliminação de registos não deve ser possível.	0
		5	Anotar quaisquer modificações à configuração do sistema de registo central.	0
		6	Criar alertas e relatórios automáticos, para eventos suspeitos ou invulgares.	0

Figura 28: Conformidade de Mapeamento do Controlo 1.2.18

Identificador	Nome	Item	Ações	44 /18
1.2.44	Manter e Monitorizar os Registos	1	Assegurar que a funcionalidade de registo de atividades, está ativa nos sistemas de *hardware* e *software*, de proteção / deteção (e.g., *firewalls*, antivírus.	0
		2	Os registos devem ser alvo de cópia de segurança e guardados, no mínimo, um ano; alguns tipos de informação podem ter de ser retidos por um período não inferior a seis anos (e.g., registos clínicos de pacientes).	0
		3	Haver um profissional de cibersegurança, que reveja os registos, à procura de tendências invulgares ou indesejadas.	0

Figura 29: Conformidade de Mapeamento do Controlo 1.2.44

Identificador	Nome	Item	Ações	22 p/ 30	22 p/ 34
1.5.22	Aplicar o Princípio do Menor Privilégio	1	Perceber o nível mínimo de permissões necessárias, para todos os	0	1
		2	Compreender as permissões atribuídas a funções dentro de cada sistema. Isto permite saber, se um utilizador com essa função, tem as permissões certas	0	0
		3	Visão completa das permissões e funções que cada utilizador tem para cada	0	0
		4	Conhecer a totalidade dos sistemas na organização e como os utilizadores os acedem, quer através da *interface* frontal de uma aplicação, quer através da infraestrutura de suporte. Isto inclui contas de utilizador em uso, e contas de	0	0
		5	Identificar as permissões de que um utilizador necessita antes de atribuir ou	0	0
		6	Rever os acessos dos utilizadores para garantir, que mantêm o menor nível de permissões necessárias para o seu trabalho.	0	0
		7	Identificar a ocorrência de mudanças, que podem obrigar a realização de alterações nas permissões, funções ou utilizadores de um sistema.	0	0
		8	Remover utilizadores que já não são necessários.	0	0
		9	Atribuir contas separadas a utilizadores que necessitem de permissões administrativas ou sensíveis. Uma conta tem as permissões administrativas, e	0	0
		10	Registar as ações tomadas pelos utilizadores administrativos e enviar os eventos para um repositório central para análise e alerta. Configurar regras de envio de notificações, quando ações inesperadas acontecem, tais como,	0	0

Figura 30: Conformidade de Mapeamento do Controlo 1.5.22

Identificador	Nome	Item	Ações	30 p/ 22	30 p/ 34
1.5.30	Identificar e Controlar quem tem acesso à Informação de Negócio	1	Determinar quem deve ter acesso à informação de negócio e se uma chave, privilégio administrativo ou palavra-passe é necessária.	0	0
		2	Não permitir desconhecidos ou pessoas não autorizadas, a terem acesso físico a qualquer um dos computadores empresariais. Inclui pessoal de limpeza e manutenção.	0	0
		3	Não permitir pessoal de reparação de computadores ou rede, trabalhar em sistemas ou dispositivos sem supervisão.	0	0
		4	Nenhuma pessoa não reconhecida, deve poder entrar no espaço de escritório, sem ser questionada por um funcionário.	0	0
		5	Trancar fisicamente os computadores portáteis e outros dispositivos móveis, quando não estão a ser utilizados.	0	0
		6	Utilizar a funcionalidade de bloqueio de sessão, incluída em nos sistemas operativos, que bloqueia o ecrã, se o computador não for utilizado durante um período de tempo especificado (por exemplo, 2 minutos).	0	0
		7	Utilizar um ecrã de privacidade ou posicionar a tela de cada computador, para não se conseguir ver a informação no ecrã, por quem passe nas proximidades.	0	0

Figura 31: Conformidade de Mapeamento do Controlo 1.5.30

Identificador	Nome	Item	Ações	34 p/ 22	34 p/ 30
1.5.34	Limitar o Acesso do Colaborador a Dados e Informação	1	Restringir o acesso a sistemas e informação, ao mínimo necessário, à execução das tarefas corporativas, por parte de cada utilizador.	1	0
		2	Impossibilitar, que somente um indivíduo, incluíndo executivos e gestores séniores, inicie e aprove uma transação, seja ela financeira ou outra.	0	0
		3	Assegurar, na saída de um colaborador, que o mesmo não tenha mais acesso à informação de negócio e a sistemas.	0	0

Figura 32: Conformidade de Mapeamento do Controlo 1.5.34

Identificador	Nome	Item	Ações	19 p/ 28
1.6.19	Ciclo de Vida dos Ativos	1	*Registar todos os ativos de sistema, incluindo software e hardware.*	3
		2	Registar todos os novos ativos aquando da sua aquisição ou	3
		3	Todos os ativos são objeto de parametrizações de robustez antes de serem utilizados, sendo mantidos regularmente com atualizações e correções.	0
		4	Ativos que se aproximam do fim de vida ou do fim de suporte por parte do fornecedor, têm um plano de desmantelamento antes de se tornarem sistemas	0
		5	Os ativos desativados são removidos do meio envolvente e destruídos em	0

Figura 33: Conformidade de Mapeamento do Controlo 1.6.19

Identificador	Nome	Item	Ações	28 p/ 19
1.6.28	Elaborar um Inventário de Informação	1	*Identificar a tecnologia, i.e., hardware e software, usada para armazenar, aceder, processar e transmitir os diversos tipos de informação.*	0
		2	Incluir a marca, modelo, números de série, e outras informações de	0
		3	Todos os tipos de informação devem ter, pelo menos, uma tecnologia de *hardware / software* listada. Quando aplicável, incluir tecnologias fora do negócio (por exemplo, "a nuvem") e quaisquer tecnologias de proteção	1
		4	Rastrear a localização de cada tipo de informação.	0
		5	Associar o dono da tecnologia, se aplicável.	0
		6	Determinar o impacto global potencial da informação.	0
		7	Atualizar o inventário, pelo menos anualmente.	0

Figura 34: Conformidade de Mapeamento do Controlo 1.6.28

Identificador	Nome	Item	Ações	7 p/ 8	7 p/ 16	7 p/ 57
1.9.7	Autenticação Baseada em Segredos	1	Todas as contas de utilizadores obrigam à utilização de um mecanismo de	0	0	0
		2	Atribuir credencias únicas a cada utilizador.	0	0	0
		3	Bloquear o dispositivo após, no máximo, 10 tentativas falhadas de	0	0	0
		4	Estrangular (*throttling*) o ritmo das tentativas de acesso. O Tempo de espera entre cada tentativa falhada aumenta. Não se deve permitir mais de 10	0	0	0
		5	Cada senha deve ter no mínimo 12 caracteres, sem restrições em relação ao	0	0	0
		6	Cada senha deve ter no mínimo 8 caracteres, sem restrições em relação ao tamanho máximo, e uso automático de bloqueio de palavras-chave, aplicando	0	0	0
		7	Educar os utilizadores a evitar escolher senhas fracas e comuns, e optar por	0	0	0
		8	Utilizar um gestor de senhas.	0	0	6
		9	Não obrigar à expiração das palavras-passe.	0	0	0
		10	Não forçar requisitos de complexidade dos segredos.	0	0	0
		11	Existir um processo de troca da palavra-passe, se o utilizador suspeitar ou	0	0	0

Figura 35: Conformidade de Mapeamento do Controlo 1.9.7

Identificador	Nome	Item	Ações	8 p/ 7	8 p/ 16	8 p/ 57
1.9.8	Autenticação Baseada em Múltiplos Fatores	1	Contas de administração dos dispositivos devem usar mais do que um fator.	0	1	0
		2	Contas acessíveis a partir da internet (e.g., autenticação em serviços na nuvem) devem sempre usar mais do que um fator.	0	1	0
		3	Cada senha deve ter no mínimo 8 caracteres, sem restrições em relação ao	0	0	0
		4	Utilização de *sms* como segundo fator, somente se não existir alternativas, como, aplicação num telemóvel corporativo ou *token* físco.	0	2	0

Figura 36: Conformidade de Mapeamento do Controlo 1.9.8

Identificador	Nome	Item	Ações	16 p/ 7	16 p/ 8	16 p/ 57
1.9.16	Implementar Autenticação Múltiplos Fatores	1	Todos os serviços administrativos, sistemas voltados para a internet e outros sistemas críticos para a organização, exigem aos utilizadores a utilização de	0	1 2	0
		2	Os métodos de *MFA* utilizados não têm vulnerabilidades conhecidas e não são depreciados por organismos de configuração padrão (e.g., *NIST*).	0	4	0
		3	Para os sistemas geridos e detidos pela organização, o módulo de autenticação *MFA* é mantido atualizado. Quaisquer dependências relacionadas do módulo são também mantidas atualizadas. A infraestrutura	0	0	0
		4	Alterações de configurações e políticas relativas ao *MFA* e tentativas de autenticação suspeitas, negadas ou de contorno, são registadas e	0	0	0

Figura 37: Conformidade de Mapeamento do Controlo 1.9.16

Identificador	Nome	Item	Ações	57 p/ 7	57 p/ 8	57 p/ 16
1.9.57	Usar Palavras-passe Fortes	1	As boas senhas consistem numa sequência aleatória de letras (maiúsculas e minúsculas), números, e caracteres especiais, e têm pelo menos 12 caracteres.	0	0	0
		2	Para sistemas ou aplicações com informações importantes, utilizar múltiplas formas de identificação (chamada autenticação "multifactor" ou "fator	0	0	0
		3	Muitos dispositivos vêm com palavras-passe de administração padrão; estas devem ser alteradas	0	0	0
		4	Considerar a possibilidade de configurar os sistemas e dispositivos, para exigir aos utilizadores, que alterem as suas palavras-passe a cada 3 meses, se	0	0	0
		5	As senhas para dispositivos e aplicações, que lidam com informação	0	0	0
		6	Utilizar uma aplicação de gestão de senhas, que cifre todas as palavras-passe armazenadas, utilize uma senha mestra forte, trocada regularmente.	8	0	0

Figura 38: Conformidade de Mapeamento do Controlo 1.9.57

Identificador	Nome	Item	Ações	9 p/ 21	9 p/ 43
1.10.9	Proteção de Código Malicioso	1	Atualização das assinaturas de código malicioso pelo menos diariamente.	0	0
		2	Acesso aos ficheiros alvo de varredura automática, incluindo quando os ficheiros são descarregados e abertos, e quando são acedidos a partir de uma	0	0
		3	*Acesso a páginas web, por um navegador, são objeto de varredura automática.*	0	0
		4	*O software previne ligações a páginas maliciosas na internet (e.g., por uma lista*	0	0
		5	*Caso de uso documentado pelo não bloqueio a páginas maliciosas na internet e o utilizador compreende e aceita o risco associado.*	0	0

Figura 39: Conformidade de Mapeamento do Controlo 1.10.9

Identificador	Nome	Item	Ações	21 p/ 9	21 p/ 43
1.10.21	Implementar Controlo Aplicacional	1	*A organização tem software instalado em todos os dispositivos, que fazem*	0	0
		2	As políticas de controlo de aplicações, são automaticamente geridas, utilizando algoritmos de aprendizagem de comportamento, entre outros. Políticas e regras também podem ser criadas e aplicadas manualmente pelos	0	0
		3	A organização impõe controlos de acesso, que permitem a aplicação das	0	0
		4	Aplicar o princípio do menor privilégio, limitando a capacidade de os utilizadores contornarem as políticas de controlo de aplicações	0	0
		5	Monitorizar as técnicas conhecidas de contorno de políticas, e incluir este conhecimento, no processo de gestão de vulnerabilidades.	0	0
		6	*O processo de robustez da configuração inicial dos sistemas, inclui a instalação de software de segurança em quaisquer novos dispositivos, i.e., estações de trabalho, servidores, computadores portáteis, dispositivos móveis, e qualquer*	0	0
		7	Os eventos das políticas de controlo de aplicações, são registados e armazenados num local central, para capturar tentativas e negações de execução de ficheiros. Os registos são configurados para desencadear alertas, que alimentam processos operacionais, tais como, a gestão de	0	0

Figura 40: Conformidade de Mapeamento do Controlo 1.10.21

Identificador	Nome	Item	Ações	43 p/ 9	43 p/ 21
1.10.43	Instalar e Atualizar Programas de Antivírus, *Spyware* e Outros *Anti-malware*	1	Instalar, utilizar e atualizar regularmente os programas antivírus e *anti-spyware* , em todos os dispositivos utilizados no negócio (incluindo computadores, telemóveis inteligentes e *tablets*).	0	0
		2	Verificar a existência de atualizações, pelo menos diariamente, ou em tempo real, se possível, e executar uma varredura completa logo a seguir.	0	0
		3	Execução de trabalho corporativo a partir de equipamentos pessoais, requer o uso de software *anti-malware* .	0	0
		4	Utilizar duas soluções antivírus de fabricantes diferentes.	0	0

Figura 41: Conformidade de Mapeamento do Controlo 1.10.43

Identificador	Nome	Item	Ações	12 p/ 15	12 p/ 36
1.11.12	Gestão das Atualizações de Segurança	1	Todo o *software* tem a atualização automática habilitada, sempre que	0	0
		2	Só são usados programas suportados pelos fabricantes.	0	0
		3	Removido dos dispositivos sempre que o período de suporte tenha caducado	0	3
		4	Isolado num ambiente separado através de uma *firewall* ou *VLAN* , bloqueando-	0	0
		5	Aplicar todos os remendos de segurança (*security patches*), incluindo, todas as configurações manuais necessárias, no prazo de 14 dias, quando: (i) a atualização é etiquetada pelo fabricante como "crítica" ou de "risco elevado"; (ii) a atualização endereça vulnerabilidades com um resultado *CVSS* de 7 ou	0	0
		6	Todos os remendos de segurança são aplicados no prazo máximo de 14 dias.	0	0

Figura 42: Conformidade de Mapeamento do Controlo 1.11.12

Identificador	Nome	Item	Ações	15 p/ 12	15 p/ 36
1.11.15	*Atualização do software e Sistemas*	1	*Dispor de uma visão completa do software no ambiente TI. Todos os dias, é possível se saber que novo software é adicionado e quais são os atuais níveis de*	0	0
		2	Atualizar todos os sistemas com as últimas correções.	0	1
		3	*Possuir uma estratégia abrangente de gestão de correções, que abranja todo o software dos sistemas: identificação, prioritização, agendamento, testes, e*	0	0
		4	Existir um processo de correção, na sua maioria automatizado, que incluía a automatização da notificação, identificação, transferência, verificação, *packaging* , salvaguarda, testes, e implementação de correções. As ações que	0	0
		5	Reavaliar a cada ciclo de correção, o risco de se realizar ou não a correção,	0	
		6	Existir documentação de apoio e informação à disposição dos utilizadores da organização, para os informar sobre a estratégia e a importância da	0	0
		7	Compreender o risco associado aos atuais níveis de remendo do ambiente TI da organização e trabalhar para mitigar o risco.	0	0

Figura 43: Conformidade de Mapeamento do Controlo 1.11.15

Identificador	Nome	Item	Ações	36 p/ 12	36 p/ 15
1.11.36	Atualização de Sistemas Operativos e Aplicações	1	*Atualizar e corrigir todo o software, em cada dispositivo corporativo.*	0	2
		2	Instalar somente as aplicações necessários ao negócio.	0	0
		3	*Ter apenas software com versão atualizada e suportada pelo fabricante.*	3	0
		4	*Na aquisição de novos computadores ou software, verificar se existem*	0	0
		5	Assignar um dia por mês, para procurar atualizações.	0	0
		6	Usar um produto que varra os sistemas e notifique caso haja atualizações	0	0

Figura 44: Conformidade de Mapeamento do Controlo 1.11.36

Identificador	Nome	Item	Ações	2 p/ 3	2 p/ 37
1.14.2	Proteção de Perímetro	1	Modificar as senhas administrativas por defeito para alternativas mais robust	1	3
		2	Desabilitar o acesso remoto administrativo.	2	0
		3	*Prevenir o acesso à interface de administração, usada na gestão de configuração*	3	0
		4	Em caso de necessidade de acesso à consola de gestão a partir da *internet*, documentar o caso de uso e proteger a interface através de autenticação multifator ou usando uma lista restrita de endereços IP em adição a um	4	0
		5	Bloquear ligações de entrada não autenticadas por defeito.	5	0
		6	*Assegurar e documentar a aprovação das regras de entrada da firewall, incluindo o caso de uso, por um indivíduo autorizado.*	6	0
		7	*Remover ou desabilitar regras de firewall não necessárias de modo expedito.*	7	0

Figura 45: Conformidade de Mapeamento do Controlo 1.14.2

Identificador	Nome	Item	Ações	3 p/ 2	3 p /37
1.14.3	*Software Firewall*	1	Modificar as senhas administrativas por defeito para alternativas mais robust	1	3
		2	Desabilitar o acesso remoto administrativo.	2	0
		3	*Prevenir o acesso à interface de administração, usada na gestão de configuração*	3	0
		4	Em caso de necessidade de acesso à consola de gestão a partir da *internet*, documentar o caso de uso e proteger a interface através de autenticação multifator ou usando uma lista restrita de endereços IP em adição a um	4	0
		5	Bloquear ligações de entrada não autenticadas por defeito.	5	0
		6	*Assegurar e documentar a aprovação das regras de entrada da firewall, incluindo o caso de uso, por um indivíduo autorizado.*	6	0
		7	*Remover ou desabilitar regras de firewall não necessárias de modo expedito.*	7	0
		8	*Utilizar a firewall pré-instalada do sistema operativo em detrimento de*	0	0

Figura 46: Conformidade de Mapeamento do Controlo 1.14.3

Identificador	Nome	Item	Ações	37 p/ 2	37 p/ 3
1.14.37	*Instalar e Ativar firewalls de software e hardware em todas as Redes Corporativas*	1	*Instalar e operar uma firewall de hardware entre a rede interna e a internet.*	0	0
		2	*Garantir a existência de software antivírus instalado na firewall.*	0	0
		3	Alterar a palavra-passe de administração por defeito e regularmente.	1	1
		4	Mudar o nome de *login* da conta de administração.	0	0
		5	Instalar, usar e atualizar regularmente, uma *firewall* de *software* em todos os computadores, telemóveis e em outros dispositivos de rede, sempre que tecnicamente viável, mesmo que esteja em uso uma VPN ou um prestador de	0	0
		6	*Habilitar o registo nas firewalls de software.*	0	0
		7	*Utilizar somente uma versão da firewall de hardware ou software, que seja atualizável, autêntica, e suportada pelo fabricante.*	0	0
		8	*Assegurar que o trabalho prestado a partir de casa, também está protegido pelo uso de firewalls por hardware e software.*	0	0
		9	Instalar um IDPS na rede corporativa.	0	0

Figura 47: Conformidade de Mapeamento do Controlo 1.14.37

D

APÊNDICE D — ÂMBITO DE APLICABILIDADE

A definição do Âmbito de Aplicabilidade é de suma importância. Exceto caso existam imponderáveis a equacionar, a aplicação do SGSPI deve englobar todos os ativos — *"anything that has value to the organization"* (JTC1/SC27, 2005) — da organização. A proteção deve ser cabal e compreender a totalidade do ecossistema organizacional e não somente uma parcela do mesmo. Organizações com âmbitos inferiores ao todo, normalmente — há exceções, estão mais interessadas em conseguir ou manter uma certificação, do que proteger, efetivamente, todas as partes interessadas do negócio.

Entregáveis[1]:

Âmbito de Aplicabilidade

- *Estabelecimento dos limites do âmbito*: e.g., o SGSPI aplica-se a todos os ativos de informação usados ou suportados pela *nome_da_empresa* no decurso das suas atividades de negócio, incluindo todas as unidades de negócio, partes interessadas e localizações.
  Caso a organização não pretenda um âmbito tão global, pode-o adaptar e personalizar às suas necessidades específicas, dependendo da natureza das operações, riscos que enfrenta e objetivos de negócio ambicionados.
  Para organizações com elevada maturidade de processos ou que cobiçam o perfil Otimizado, compreender a organização e o seu contexto (e.g., histórico/apresentação da organização, contexto no qual opera, propósito, análise SWOT, questões internas/externas que enfrenta) e compreender os requisitos (e.g., legais e regulamentares) e expectativas (e.g., obrigações contratuais) das partes interessadas (e.g., clientes, utilizadores, parceiros, fornecedores, colaboradores, seguradoras, acionistas, reguladores, credores, comunicação social, agências governamentais, organismos e associações de comércio), utilizando um modelo de *Stakeholder Management*, pode ser benéfico.

1 Nota do autor: as ações autoexplicativo estão suprimidas.

- *Determinar os ativos no limite definido*: a decifração desta ação, está intimamente ligada à anterior. No entanto, a lista ulterior é uma excelente base inicial de reflexão:
  - Clientes: e.g., por perfil, segmentação;
  - *Hardware*: e.g., servidores, portáteis, impressoras, telemóveis, discos amovíveis, equipamento de rede;
  - Infraestrutura: e.g., edifícios, escritórios;
  - Informação: e.g., formato papel, suporte eletrónico — base de dados, folhas de cálculo, ficheiros em formato PDF;
  - Intangíveis: e.g., reputação, marca, URL, IP;
  - Pessoas: e.g., colaboradores, trabalhadores temporários, estagiários, voluntários;
  - Prestadores de serviço: e.g., nuvem — AWS — `https://aws.amazon.com/`, *gmail* -`https://mail.google.com/`, limpeza, jurídico, serviços públicos essenciais — eletricidade, água;
  - *Software*: e.g., programas comerciais, *open-source*, *shareware*, *Software Bill of Materials*.

  Ver o anexo R.

Realizar Melhorias a Processos / Procedimentos / Tecnologias

- *Avaliar regularmente os processos, procedimentos e soluções tecnológicas conforme os riscos identificados*: constatar o apêndice V.
- *Realizar treinos ou exercícios table-top, que simulem ou executem passo a passo um cenário de um evento principal, de modo a identificar potenciais fraquezas nos processos, procedimentos, tecnologia, ou prontidão do pessoal*: observar o apêndice X.

E

APÊNDICE E — *FIREWALL*

As ferramentas de proteção de perímetros, são essenciais no controlo e monitorização do tráfego de entrada e saída, assegurando a segurança e integridade dos ativos da rede corporativa, face a ameaças cibernéticas. Além disso, previnem acessos não autorizados, otimizam e priorizam o tráfego, e aumentam a produtividade bloqueando o acesso a conteúdos indesejáveis.

Entregáveis[1]:

- *Em caso de necessidade de acesso à consola de gestão a partir da internet, documentar o caso de uso e proteger a interface, via autenticação multifator ou usando uma lista restrita de endereços IP, em adição a um mecanismo de gestão de senhas fiável*: constatar o apêndice P.
- *Assegurar e documentar a aprovação das regras de entrada da firewall, incluindo o caso de uso, por um indivíduo autorizado*: este requisito assegura-se pelo preenchimento da tabela posterior e aceitação por parte do responsável de negócio, segurança ou dono do ativo *firewall*. O requerente não pode aprovar para se garantir o princípio dos "quatro olhos"[2] — para uma determinada atividade, decisão ou transação ser executada, tem de ser aprovada no mínimo por duas pessoas. O canal de comunicação/aprovação deve ser não verbal, por exemplo, utilizando uma mensagem de correio eletrónico, para gerar a necessária evidência.

Tabela 78: Documento de Alteração das regras da *firewall*

Origem	Protocolo	Porto	Destino	Data de Alteração	Motivo
172.20.1.0/26	TCP	1500	10.198.33.0/25	10.02.2023	Permitir fluxo de replicação de dados do servidor.

O número de campos da tabela pode ser adaptado às necessidades específicas da organização. Antes de ser aprovada a inclusão de uma nova regra ter atenção a configurações desviantes:

  - Protocolos inseguros, e.g., HTTP, *telnet*.

1 Nota do autor: as ações autoexplicativo estão suprimidas.
2 *Four eyes principle* na designação anglo-saxónica.

  - Blocos de grande dimensão, e.g., /16.
  - Portos tendencialmente vulneráveis, e.g., 445, 8080.

- *Instalar e operar uma firewall de hardware entre a rede interna e a internet*: a solução a escolher deve conter o maior número de funcionalidades e características (Stanfield, 2019; SunnyValleyNetworks, s.d.; TeachComputerScience, s.d.) da seguinte lista:
  - Monitorização e controlo de largura de banda disponível (e.g., priorizar aplicações, tráfego de *backup*).
  - Capacidade de filtragem *web*.
  - Agregação de *links* e SD-WAN.
  - Acesso a *logs*.
  - *Sandboxing*: efetivo na proteção contra ameaças dia zero e mensagens de correio eletrónico com anexos e URL suspeitos.
  - Controlador de rede sem fios integrado.
  - *Deep Packet Inspection* e filtragem de pacotes.
  - *Virtual Private Network*.
  - Filtragem de *malware* e vírus.
  - *Intrusion Prevention System*.
  - Integração de gestão de identidades e *Single Sign On*.
  - Controlo aplicacional e de utilizadores (e.g., prevenir aplicações não confiáveis de executarem qualquer função).
  - *Multi-Tenancy*.
  - Garantir que o fornecedor tem um plano de atualização frequente disponível.
  - Ter sempre o licenciamento ativo.
  - Considerar solução de virtualização em ambiente nuvem.
  - *What Is Unified Threat Management*: algumas das características supraditas estão incluídas nesta funcionalidade agregadora.
  - Ser escalável/modular à medida que o número de ativos e infraestrutura a ser protegida aumenta.
  - Integração com a solução de gestão de identidades em vigor.

  - Alta disponibilidade: por exemplo, a *firewall* principal pode ser física e a redundante virtual.
  - Disponibilização de diferentes configurações e políticas: e.g., permitir a passagem de tráfego autorizado que cumpra um conjunto de regras.

- *Instalar um IDPS na rede corporativa*: optar por uma solução com as funcionalidades ulteriores:
  - Detetar e analisar o tráfego de rede em tempo real.
  - Múltiplos métodos de deteção: e.g., baseados em assinatura, comportamento, anomalias, heurística.
  - Consola de gestão centralizada.
  - Responder automaticamente a ameaças através do bloqueio ou quarentena de tráfego malicioso, ou a partir de outras ações pré-definidas.
  - Integração com outras ferramentas de segurança: e.g., *firewall*, *software* antivírus, *Security Information and Event Management*.
  - Políticas personalizáveis.
  - Escalabilidade.
  - Fornecer registos e relatórios detalhados, que possam ser utilizados na investigação de incidentes e para fins de conformidade.
  - Atualizado regularmente.
  - Ser suportado pelo fabricante.
  - Considerar solução de virtualização em ambiente nuvem.

APÊNDICE F — ROBUSTEZ DA CONFIGURAÇÃO, VULNERABILIDADES E INTRUSÃO

Configurar robustamente os sistemas, é uma das atividades fundamentais na área da segurança cibernética, pela eliminação de potenciais vetores e superfície de ataque, através da remoção e parametrização de serviços, portos, permissões, contas, entre outras componentes. Os testes de vulnerabilidade e intrusão, funcionam como autênticos aferidores do grau de qualidade das configurações efetuadas.

Entregáveis[1]:

Robustez da Configuração Inicial do Sistema

Existem disponíveis uma panóplia diversificada de *templates*, que podem e devem ser usados na configuração e parametrização inicial e contínua dos sistemas. Estes modelos fornecem um ótimo ponto de partida:

- *Center for Internet Security Benchmarks*[2]: são amplamente reconhecidos e fornecem orientações precisas de como robustecer os sistemas operativos, aplicações e dispositivos de rede. Estão disponíveis para uma variedade de plataformas, incluindo *Windows*, *Linux*, *macOS* e dispositivos móveis.
- *Defense Information Systems Agency Security Technical Implementation Guides*[3]: inclui configurações específicas para múltiplos sistemas, satisfazendo os requisitos de segurança do *Department of Defense*.
- *Microsoft Security Baselines*[4]: recomendações de configuração de segurança para o *Windows* e outros produtos *Microsoft*.
- *Agence Nacionale de la Sécurité des Systèmes d'Information — Configuration recommendations of a GNU/Linux system*[5]: foco em diretrizes genéricas de configuração de sistemas e em princípios basilares, que devem ser aplicados na configuração inicial.

1 Nota do autor: as ações autoexplicativo estão suprimidas.
2 https://learn.cisecurity.org/benchmarks
3 https://www.stigviewer.com/stigs
4 https://techcommunity.microsoft.com/t5/microsoft-security-baselines/bg-p/Microsoft-Security-Baselines
5 https://www.ssi.gouv.fr/en/guide/configuration-recommendations-of-a-gnulinux-system/

- *Awesome-security-hardening*[6]: uma coleção de fantásticos guias de robustez da segurança, melhores práticas, listas de verificação, referências, ferramentas e outros recursos.

Executar Varredura de Vulnerabilidades

Existe uma enorme panóplia de ferramentas gratuitas, que podem ser usadas, sem vastos conhecimentos técnicos, na deteção de vulnerabilidades. O autor inúmera algumas das que costuma utilizar, sendo uma ótima base na edificação de um robusto programa de vulnerabilidades:

- *Burp Suite*[7]: execução de testes de segurança em aplicações.
- *Nessus*[8]: a versão de comunidade permite verificar até 16 IP por varredura.
- *Nmap*[9]: utilitário de segurança usado na identificação e auditoria de ativos de rede.
  Como exemplo, a execução do comando *nmap -script vuln IP*, permite detetar vulnerabilidades conhecidas.
- *OpenVas*[10]: executa mais de cinquenta mil testes na identificação de vulnerabilidades na rede e aplicações.

A execução de uma ou mais das ferramentas supraditas, deve-o ser de frequência regular, no mínimo trimestral. Pelo menos as vulnerabilidades etiquetadas como críticas, severas ou de alto impacto, carecem de remediação num espaço temporal diminuto (e.g., 30 dias).

Conduzir Teste de Intrusão

A execução de um *pentesting* exige, normalmente, o recurso a profissionais. A próxima lista contém os pontos a serem tidos em consideração na elaboração do contrato:

- Definir o âmbito do teste de intrusão.
- Ajustar o prazo de execução dos testes.
- Determinar o tipo de teste a ser executado (e.g., externo, interno, com/sem conhecimento da rede).
- Os testes devem incluir os cenários: (i) autenticação, (ii) autorização, (iii) encriptação, (iv) exfiltração, (v) negação de serviço.

6 https://github.com/decalage2/awesome-security-hardening/
7 https://portswigger.net/burp/communitydownload
8 https://www.tenable.com/products/nessus/nessus-essentials
9 https://nmap.org/
10 https://github.com/greenbone/openvas-scanner

- Garantir que nas vulnerabilidades descobertas recorrendo a ferramentas automáticas, é entregue uma prova de conceito[11].
- Documentar o processo empregue, as evidências encontradas e recomendações de mitigação e melhoria.
- Remover possíveis artefactos pós-condução dos testes.

11 *Proof of concept* na denominação anglo-saxónica.

G

APÊNDICE G — DESBLOQUEIO SEGURO DO SISTEMA

O desbloqueio seguro do sistema é parte integrante do processo de gestão de identidades e autorização, sendo fulcral na preservação da tríade CIA nos variados recursos organizacionais, nomeadamente na contribuição contra a usurpação de identidade.

Entregáveis[1]:

- *Bloquear o dispositivo após, no máximo, 10 tentativas falhadas de autenticação* e *Estrangular (throttling) o ritmo das tentativas de acesso. O Tempo de espera entre cada tentativa falhada aumenta. Não se deve permitir mais de 10 tentativas num espaço temporal de 5 minutos*:
  - Para os sistemas *Linux* instalar e utilizar o pacote *fail2ban*[2].
  - Nos sistemas *Windows* configurar no editor de GPO a *Account Lockout Policy* em `Computer Configuration > Windows Settings > Security Settings > Account Policies > Account Lockout Policy`.

  É importante testar a política, assegurando ser eficaz, e não resulta em bloqueios desnecessários. Deve também ser assegurado de que os utilizadores estão cientes da política e das suas implicações.
- *O segredo usado somente no ato de desbloqueio deve ter pelo menos 6 caracteres*:
  - Para os sistemas *Linux* não existe a característica de GPO. A implementação de requisitos em segredos pode ser conseguida utilizando algumas alternativas:
    * *Pluggable Authentication Modules*: conjunto de módulos para autenticação, incluindo políticas de *passwords*.
    * Ficheiro de configuração `/etc/login.def`: definições de contas de utilizadores e políticas de senhas.

1 Nota do autor: as ações autoexplicativo estão suprimidas.
2 https://github.com/fail2ban/fail2ban

* Utilizar ferramentas de terceiros, e.g., o módulo *pam_cracklib*[3] , *pam_tcb*[4].

Os sistemas *Linux* têm múltiplos mecanismos de autenticação e ficheiros de segredos, e.g., */etc/passwd*, */etc/shadow*, */etc/group*, sendo importante rever e configurar os parâmetros de todos os ficheiros e módulos, assegurando a consistência da política de *passwords* em todo o sistema. Importa também referir, que muitas distribuições de *Linux*, têm ferramentas próprias relacionadas com a gestão de segredos, sendo necessário a sua consulta, de modo a garantir uma configuração apropriada.

– Nos sistemas *Windows* abrir o editor de GPO e criar uma política específica para senhas em `Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy`.

3 https://www.tenable.com/audits/items/CIS_Debian_Linux_7_v1.0.0_L1.audit:67b87807788470cd6e6df619ecd0c68d

4 https://man.linuxreviews.org/man8/pam_tcb.8.html

H

APÊNDICE H — CICLO DE VIDA DAS CONTAS DOS UTILIZADORES

O processo de gestão das contas de utilizador, níveis de acesso e permissões aos diferentes recursos, assegura a confidencialidade, rastreabilidade e conformidade face a diferentes regulações e requisitos legais.

Entregáveis[1]:

- *Processo de criação e aprovação da conta do utilizador*: consiste num conjunto de passos:
  - Pedido de criação da conta de utilizador: submeter via sistema de suporte TI, preferencialmente, ou via pedido escrito (e.g., mensagem de correio eletrónico), pelo departamento de RH ou através do responsável direto a quem esse utilizador responde. Existe um conjunto de atributos a serem fornecidos juntos à solicitação:
    * Nome completo do utilizador.
    * Função/papel a desempenhar.
    * Início e término de funções.
    * Departamento.
    * Responsável hierárquico.
    * Acessos e permissões iniciais necessárias, devendo estar previamente aprovadas, pelo dono de cada ativo. Sem essa validação, o utilizador é criado sem a atribuição de quaisquer privilégios nos diferentes sistemas.
  - Autenticação secreta: a senha inicial é criada aleatoriamente, conforme as regras da organização, preferencialmente, via uma ferramenta para esse efeito. Essa palavra-passe expira após o primeiro acesso e o utilizador é forçado a criar uma.

1 Nota do autor: as ações autoexplicativo estão suprimidas.

  - Informação ao utilizador: após a criação da conta, o utilizador é informado presencialmente ou via telefone e a senha inicial é transmitida pelos canais de comunicação descritos.
  - Ajustes de permissões: o utilizador sempre que precisar de aceder a um novo sistema, deve solicitar o acesso ao dono do ativo, via canal oficial estabelecido na organização, normalmente o correio eletrónico ou a aplicação de suporte. O responsável por cada recurso deve, pelo menos anualmente, identificar:
    * Utilizadores sem necessidade de terem acesso (e.g., saída, mudança de função).
    * Contas de utilizadores sem identificação adequada, e.g., contas genéricas, contas partilhadas sem responsável definido.
    * Contas com permissões excessivas para a função.
    * Utilizadores com função desajustada.
  - Remoção do utilizador: informação de saída é comunicada pelo responsável direto ou departamento de RH ao suporte de TI atempadamente, indicado a data na qual a conta deve ser desabilitada. A mesma é removida após conclusão do processo de saída e verificação de não impacto em nenhum dos sistemas.

- *Usar conta separada no desempenho de atividades privilegiadas*: a conta privilegiada deve identificar o utilizar(e.g., miguel.soares_admin) e não ser genérica (e.g., *admin*, SA), de modo a se poder mais facilmente rastrear a execução das atividades especiais.

I

APÊNDICE I — AUTENTICAÇÃO BASEADA EM UM OU MAIS FATORES

O conceito de autenticação é um elemento essencial, na proteção da informação e recursos de acessos indevidos, pelo processo de verificação da identidade do utilizador, sistema ou dispositivo. É um dos processos utilizados na prevenção de ataques de usurpação de identidade e garante de *accountability* por permitir rastrear quem acede a um recurso ou serviço e quando.

Entregáveis[1]:

Autenticação Baseada num Fator

- *Bloquear o dispositivo após, no máximo, 10 tentativas falhadas de autenticação* e *Estrangular (throttling) o ritmo das tentativas de acesso. O Tempo de espera entre cada tentativa falhada aumenta. Não se deve permitir mais de 10 tentativas num espaço temporal de 5 minutos*: verificar o apêndice G.
- *Cada senha deve ter no mínimo 12 caracteres, sem restrições relativamente ao tamanho máximo*, *Cada senha deve ter no mínimo 8 caracteres, sem restrições relativamente ao tamanho máximo, e uso automático de bloqueio de palavras-chave, aplicando uma lista de negação* e *As boas senhas consistem numa sequência aleatória de letras (maiúsculas e minúsculas), números, e caracteres especiais, e têm pelo menos 12 caracteres*: observar o apêndice G. Adicionalmente nos sistemas *Windows* a instalação do módulo *Azure AD Password Protection for Windows Server Active Directory*[2] previne o uso de palavras-passe fracas. Em relação aos ambientes *Linux*, o pacote *pam_cracklib*[3] verifica se a escolha do segredo por parte do utilizador é suficientemente robusta.
- *Educar os utilizadores a evitar escolher senhas fracas e comuns, e optar por segredos de tamanho longo*: os gestores de segredos normalmente incorporam a funcionalidade de averiguar a qualidade da palavra-passe. Conferir o apêndice P.

1 Nota do autor: as ações autoexplicativo estão suprimidas.
2 https://www.microsoft.com/en-us/download/details.aspx?id=57071
3 https://manpages.debian.org/stretch/libpam-cracklib/pam_cracklib.8.en.html

A entropia[4] é a medida, que permite verificar quão aleatório e imprevisível é uma senha. A fórmula matemática de cálculo da entropia, consiste em $log_2 N^L$, onde o N é o número de possíveis caracteres e o L é o tamanho da palavra-passe. Quanto maior é a entropia, mais seguro e difícil de quebrar é o segredo. O valor nunca deve ser inferior a 60 BIT.

- *Utilizar um gestor de senhas* e *Utilizar uma aplicação de gestão de senhas, que cifre todas as palavras-passe armazenadas, utilize uma senha mestra forte, trocada regularmente*: observar o apêndice P.
- *Existir um processo de troca da palavra-passe, se o utilizador suspeitar ou souber de comprometimento da mesma*: averiguar o apêndice J.

Autenticação Baseada em Múltiplos Fatores

- *Contas de administração dos dispositivos devem usar mais do que um fator*: nos sistemas *Linux* uma maneira fácil e eficiente é combinando a instalação do *Google Authenticator PAM module*[5] com um *OTP-generator*[6].
  Em relação ao ambiente *Windows* passa por instalar a aplicação *Microsoft Authenticator*[7] e configurar o *Azure AD Multi-Factor Authentication*[8], independentemente se o cenário é *cloud-only*, híbrido ou *on-premise*.
- *Contas acessíveis a partir da internet (e.g., autenticação em serviços na nuvem) devem sempre usar mais do que um fator*: todos os fornecedores de soluções na *internet* incorporam soluções de autenticação múltiplos fatores (e.g., *Azure Active Directory Free*[9]) ou permitem a integração com sistemas de identidade de terceiros (e.g., *Ping Identity*[10]).
- *Cada senha deve ter no mínimo 8 caracteres, sem restrições relativamente ao tamanho máximo*: consultar o apêndice G.
- *Alterações de configurações e políticas relativas ao MFA e tentativas de autenticação suspeitas, negadas ou de contorno, são registadas e armazenadas num local de registos central*: constatar o apêndice Q.

4 https://www.pleacher.com/mp/mlessons/algebra/entropy.html
5 https://github.com/google/google-authenticator-libpam
6 https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2
7 https://www.microsoft.com/en-us/security/mobile-authenticator-app
8 https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted
9 https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-pricing
10 https://www.pingidentity.com/en/platform/capabilities/multi-factor-authentication.html

J

APÊNDICE J — FORMAR OS COLABORADORES

É um dizer comum, mas os colaboradores e as restantes partes interessadas de uma organização, são o elo mais permissivo na edificação e manutenção de um programa de segurança e privacidade da informação, e consequentemente é fulcral tornar-se a parte central do processo, via uma sensibilização e consciencialização regular, nas temáticas de cibersegurança.

Entregáveis[1]:

- *Formar os utilizadores imediatamente quando contratados e pelo menos uma vez por ano, posteriormente, sobre as políticas de segurança da informação e o que se espera que façam para proteger a informação e tecnologia do negócio*: todos os colaboradores, nas suas respetivas áreas, necessitam de saber como aplicar os diferentes requisitos de segurança e privacidade da informação para proteger os ativos da organização. O autor recomenda a criação de uma Carta de Condução sobre Segurança e Privacidade da Informação. O programa é constituído por uma formação e consequentemente por um exame de avaliação de conhecimentos, resultante na emissão da "Carta de Condução", em caso de aproveitamento igual ou superior a uma determinada percentagem, ou valor, a ser definida pela organização. Sem este certificado, o colaborador não está habilitado a manipular ativos de informação da organização. O requisito de aproveitamento na "Carta de Condução" é adicionado ao descritivo de competências de todas as funções. O certificado é válido por um ano, tendo de ser renovado por iguais períodos.
  O treino é constituído por um conjunto de módulos customizados à função desempenhada. Como exemplo, consideremos o Dono de Ativo (*Asset Owner*). Neste caso, estamos perante indivíduos que são responsáveis (*accountable*) por um ou mais ativos da organização. Os seguintes módulos podem fazer parte do treino:
  - Gestão de Ativos para Donos de Ativos;
  - Gestão de Fornecedores;

1 Nota do autor: as ações autoexplicativo estão suprimidas.

- Documentar Registos de Processos de Segurança;
- Monitorizar e Rever Processos de Segurança.

O ponto a reter é, que nenhum indivíduo deve ou pode processar e tratar dados e informação corporativa sem estar devidamente sensibilizado e consciencializado nas temáticas de cibersegurança.

Há um inúmero substancial de repositórios de informação com conhecimento fidedigno e sem custos, que podem servir de suporte à construção do programa:

- `https://learnsecurity.amazon.com/en/index.html`;
- `https://protectconnect.com/en/index.html`;
- `https://skillsforall.com/career-path/cybersecurity`.

No entanto, a organização deve-se basear sobretudo nos seus processos internos e extrair dos mesmos, a maioria do conteúdo.

- *Assegurar que assinam uma declaração, onde se comprometem a seguir as políticas instituídas, e que compreendam as penalidades em caso contrário.*: observar o apêndice W.
- *Incluir nos treinos, cenários de emergência ou incidentes de segurança, como tratar a informação dos clientes e de negócio, e de que modo se podem usar os computadores e telemóveis corporativos.*: constatar os apêndices W e X.

APÊNDICE K — PROTEÇÃO DE CÓDIGO MALICIOSO

Existe uma panóplia diversificada de vírus e *malware*, que se propagado por múltiplos meios, como anexos no correio eletrónico, *downloads* maliciosos e *websites* infetados. Uma vez infetado o dispositivo, os programas maliciosos provocam danos, como exfiltração de dados pessoais, corrupção de ficheiros, falhas e mau funcionamentos, e até mesmo controlo total do equipamento. O uso de *software* preventivo é obrigatório em qualquer programa de cibersegurança.

Entregáveis[1]:

- *Caso de uso documentado pelo não bloqueio a páginas maliciosas na internet e o utilizador compreende e aceita o risco associado*: indivíduos que por motivos profissionais necessitem de acesso irrestrito ao espaço digital, devem assinar um documento anuindo os riscos e responsabilidade. Esses grupo de utilizadores deve estar segregado numa rede à parte.
  Possível texto a assinar em como compreende e toma consciência: «Ao aceder à *internet* através deste canal corporativo, reconhece e concorda que é o único responsável pela sua atividade em linha. Este canal proporciona acesso ilimitado à navegação no espaço digital, e o utilizador compreende que pode encontrar conteúdos inadequados, ofensivos, ou potencialmente prejudiciais. A *nome_da_empresa* não se responsabiliza por quaisquer danos ou prejuízos que resultem da utilização da *internet* através deste canal. É da responsabilidade do utilizador, utilizar a *internet* de forma responsável e legal, e tomar as devidas precauções para proteger as informações pessoais e de negócio, e os dispositivos contra ameaças cibernéticas. Ao utilizar este canal de acesso não condicionado, o utilizador concorda em cumprir todas as leis e regulamentos aplicáveis, e em respeitar os direitos, liberdades e privacidade de terceiros.»
- *Instalar, utilizar e atualizar regularmente os programas antivírus e anti-spyware, em todos os dispositivos utilizados no negócio (incluindo computadores, telemóveis inteligentes e tablets)*: um programa *anti-malware* deve agregar as seguintes funcionalidades:

1 Nota do autor: as ações autoexplicativo estão suprimidas.

  - Proteção e monitorização em tempo real;
  - Remoção ou quarentena e alerta de programas maliciosos;
  - Atualização automática de componentes e definições de *malware*;
  - Varredura de correio eletrónico, incluindo anexos e URL;
  - Proteção de ameaças, como *websites* maliciosos, tentativas de *phishing* e outras ameaças em linha;
  - Restrição a categoirias de *sites*;
  - Capacidade de análise forense de modo a permitir identificar a fonte do ataque;
  - Resposta automática baseada em políticas predefinidas;
  - Integração com outras ferramentas de seguraça (e.g., *firewall*, SIEM) ;
  - Consola central de gestão;
  - Integração com *feeds* de segurança disponibilizando informações sobre as últimas ameaças e vulnerabilidades;
  - Capacidade UEBA;
  - Construção de relatórios (e.g., postura de segurança, identificação de tendências, incidentes).

  Para os sistemas *windows* utilizar o *software* que acompanha o SO de nome *Windows Security*, no caso do *Linux* o *ClamAV ®*[2] e instalar adicionalmente um EDR, como o *CrowdStrike Falcon ® Insight XDR*[3] ou o *Heimdal ® Endpoint Detection and Response*[4].

- *A transferência e uso de freeware ou shareware tem de ser avaliada em termos de suporte técnico e funcionalidades disponibilizadas*: a licença deve ser lida para evitar possíveis violações e consequentes ações legais. Como exemplo, o *software Winrar* somente permite a utilização em modo experimental durante quarenta dias[5]. Após o término o utilizador fica obrigado a adquirir uma licença.
- *Não ligar nenhum hardware desconhecido, não confiável ao sistema ou rede e não inserir nenhum CD, DVD, ou drive USB desconhecida*: configurar uma

2 https://www.clamav.net/
3 https://www.crowdstrike.com/products/endpoint-security/falcon-insight-xdr/
4 https://heimdalsecurity.com/enterprise-security/endpoint-detection-and-response-edr-software
5 https://www.win-rar.com/winrarlicense.html?&L=0

GPO a permitir ou a bloquear um determinado conjunto de identificadores de *hardware*[6].

- *Todos os utilizadores têm as macros desativadas por defeito e não as podem reativar*: ativar esta restrição recorrendo a uma GPO, que ative o parâmetro *Block macros from running in Office files from the Internet* ou caso as macros sejam necessárias, ativando *Disable all macros except digitally signed macros*[7].
- *Os registos são anotados e armazenados num local central, para capturar a execução de tipos de ficheiros com macros, tais como, .docm, .pptm, .xlsm*: conferir o apêndice Q.

6 https://learn.microsoft.com/en-us/windows/client-management/manage-device-installation-with-group-policy

7 https://www.cisecurity.org/insights/white-papers/intel-insight-how-to-disable-macros

L

APÊNDICE L — APLICAÇÕES AUTORIZADAS

O controlo aplicacional é um requisito obrigatório no garante dos direitos autorais, bem como, no combate à propagação de programas maliciosos e redução da superfície corporativa TI a ataques internos e externos.

Entregáveis[1]:

- *Somente aplicações aprovadas podem ser instaladas e executadas nos dispositivos*: várias técnicas manuais e/ou automáticas, podem ser aplicados isolada ou simultaneamente, de modo a garantir um controlo total sobre o espectro aplicacional:
  - O programa de gestão de ativos *Lansweeper* possui um relatório intitulado *Unauthorized Software Audit*[2], que permite varrer toda a rede empresarial e etiquetar cada componente como autorizada ou não aprovada;
  - Somente permitir *drivers* assinados digitalmente. Nos sistemas *Windows* a funcionalidade *Driver Signature Enforcement* é um método válido em se alcançar tal feito, configurando a GPO `User Configuration > Administrative Templates > System > Driver Installation > Code signing for devices drivers > Enabled`;
  - Utilizando a funcionalidade *Windows Defender Application Control*[3], uma organização consegue controlar as *drivers* e aplicações possíveis de serem executadas nos clientes *Windows*;
  - Não permitir aos utilizadores serem administradores locais das máquinas é em si um método eficaz;
  - Nos ambientes *Linux* as opções de desabilitar o gestor de pacotes (*package manager*) ou apenas permitir a instalação a partir de certos repositórios, remover os privilégios *sudo* aos utilizadores e restringir o uso das funcionalidades *AppArmor* e *SElinux*, são válidas.

1 Nota do autor: as ações autoexplicativo estão suprimidas.
2 https://www.lansweeper.com/report/unauthorized-software-audit/
3 https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/wdac-and-applocker-overview

- *Aplicar o princípio do menor privilégio, limitando a capacidade de os utilizadores contornarem as políticas de controlo de aplicações estabelecidas*: observar o apêndice S.
- *O processo de robustez da configuração inicial dos sistemas, inclui a instalação de software de segurança em quaisquer novos dispositivos, i.e., estações de trabalho, servidores, computadores portáteis, dispositivos móveis, e qualquer outro dispositivo, que aceda a dados organizacionais. Isto pode incluir dispositivos de propriedade da organização e BYOD*: conferir o apêndice F.
- *Os eventos das políticas de controlo de aplicações, são registados e armazenados num local central, para capturar tentativas e negações de execução de ficheiros. Os registos são configurados para desencadear alertas, que alimentam processos operacionais, tais como, a gestão de incidentes ou de alterações. Um processo de gestão de alterações de emergência é seguido, quando programas críticos são bloqueados.*: constatar o apêndice Q.
- *Todo o código, de origem desconhecida, tem de ser executado num ambiente controlado (sandbox), que previna acesso a outros recursos, exceto caso haja permissão explícita do utilizador*: em *Linux* recorrendo aos *Linux namespaces*, *AppArmor*, *SELinux* e contentores (e.g., *Docker*, LXC[4]). No **Windows** recurso à funcionalidade *Windows Sandbox*[5], virtualização (e.g., VirtualBox[6]) e contentores.

4 https://linuxcontainers.org/lxc/introduction/
5 https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-sandbox/windows-sandbox-overview
6 https://www.virtualbox.org/

M

APÊNDICE M — GESTÃO DAS ATUALIZAÇÕES DE SEGURANÇA

A gestão das atualizações de segurança são fundamentais por garantirem um ambiente seguro e estável, que esteja conforme os requisitos regulamentares, protegendo igualmente a reputação da organização. A falta de aplicação de remendos, é um dos principais vetores explorados pelos atores maliciosos, de modo a ganharem acesso aos ativos e à informação corporativa. Por outro lado, contribuem para a manutenção da estabilidade e desempenho do sistema, evitando problemas operacionais.

Entregáveis[1]:

- *Dispor de uma visão completa do software no ambiente TI. Todos os dias, é possível se saber que novo software é adicionado e quais são os atuais níveis de patch*: esta ação carece de um programa de gestão de inventário dos ativos corporativos, conforme descrito no apêndice R. O uso de uma aplicação de deteção de vulnerabilidades, analisada no apêndice F, é um excelente complemento na materialização deste ponto.
- *Existir um processo de correção, na sua maioria automatizado, que incluía a automatização da notificação, identificação, transferência, verificação, packaging, salvaguarda, testes, e implementação de correções. As ações que requerem a avaliação do risco ou a realização de avaliações, continuam a ser manuais*: existe uma panóplia de possibilidades nos ambientes *Windows* de automatizar a correção de vulnerabilidades:
  - GPO[2];
  - WSUS[3];
  - *Intune*[4];

1 Nota do autor: as ações autoexplicativo estão suprimidas.
2 https://learn.microsoft.com/en-us/windows/deployment/update/waas-wufb-group-policy
3 https://learn.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wsus
4 https://learn.microsoft.com/en-us/mem/intune/protect/windows-update-for-business-configure#windows-10-feature-updates

– *Configuration Manager*[5].

Nos sistemas *Linux*, dependendo da distribuição, existem várias opções viáveis, como:

– *Yum-Cron*[6];

– *Unattended-upgrades*[7];

– *Salt Project*[8].

É importante existir uma lista resume, com todos os tipos de ativos e a cadência de *patching*. A Tabela 79 ilustra os campos mínimos pretendidos.

Tabela 79: Listagem de *Patching*

Tipo de Recurso	**Periocidade**	**Instalação**
Portáteis	15 dias	Automática
Servidores não críticos	30 dias	Automática
Servidores críticos	60 dias	Manual
Firewalls	90 dias	Manual
(...)	(...)	(...)

- *Existir documentação de apoio e informação à disposição dos utilizadores da organização, para os informar sobre a estratégia e a importância da aplicação de correções*: observar o apêndice J.
- *Compreender o risco associado aos atuais níveis de remendo do ambiente TI da organização e trabalhar para mitigar o risco*: verificar o apêndice V.

5 https://learn.microsoft.com/en-us/mem/configmgr/osd/deploy-use/manage-windows-as-a-service
6 https://www.redhat.com/sysadmin/using-yum-cron
7 https://wiki.debian.org/UnattendedUpgrades
8 https://repo.saltproject.io/

APÊNDICE N — GESTÃO DO LICENCIAMENTO DE SOFTWARE

Uma gestão eficaz das licenças de *software*, permite não só assegurar a conformidade legal com o estipulado nos acordos de licenciamento, mas igualmente reduzir custos e *shadow* IT.

Entregáveis[1]:

- *Todo o software em utilização encontra-se licenciado*: as seguintes práticas devem ser observadas:
  - Inventório de todas as licenças compradas, em uso e disponíveis.
  - Utilizar uma ferramenta de gestão de licenciamento centralizada, que permita a geração de relatórios, estabelecimento de alertas, análises de uso e previsão de futuras necessidades.
  - Revisão periódica das licenças assignadas.
  - Negociação em volume sempre que possível.

  Dependendo dos objetivos, capacidade financeira e cenários em causa, as opções ulteriores são uma escolha válida:
  - *Fossology*[2].
  - *Lansweeper*[3].
  - *ManageEngine AssetExplorer*[4].
  - *Snipe-IT*[5].

1 Nota do autor: as ações autoexplicativo estão suprimidas.
2 https://www.fossology.org/
3 https://www.lansweeper.com/
4 https://www.manageengine.com/products/asset-explorer/
5 https://snipeitapp.com/

O

APÊNDICE O — SALVAGUARDA DOS DADOS

As salvaguardas são parte fulcral do processo de gestão estratégico dos dados, permitindo recuperar a informação de negócio, em caso de perda, corrupção ou eliminação involuntária. São peças-chave na continuidade do negócio e em questões legais e regulatórias, por garantirem a preservação dos dados durante o tempo estipulado. Devem ser armazenadas num local geográfico diferente ao de origem dos dados.

Entregáveis[1]:

- *O responsável por cada conjunto de dados toma decisões em torno da importância e dos tempos de recuperação dos mesmos (objetivos de recuperação). A equipa de TI fornece aconselhamento sobre os objetivos de recuperação*: a decisão estratégica das salvaguardas é do negócio e não das TI. A tabela sequente resume e exemplifica, a informação basilar a ser preenchida, garantindo-se um plano de salvaguardas robusto:

Tabela 80: Plano de Salvaguardas

Recurso	Frequência	A cada	Retenção	Tipo	Encriptação	Restaurar a cada	RPO	Local / Remoto
A	Diária	1h	7 Dias	Incremental	Sim	3 meses	5h	*S3 Bucket*
B	Semanal	168h	3 Semanas	Diferencial	Sim	6 meses	168h	Zona
C	Mensal	720h	5 Meses	Completo	Sim	1 ano	721h	Região

Os valores supraditas carecem de adaptação ao modelo de negócio, por parte dos gestores de negócio.

O RPO é o tempo máximo de informação a que se está disposto a perder. Tomando o exemplo em análise, a coluna do "RPO" tem de ser igual ou superior à coluna "A cada", caso contrário, em caso de disrupção, há perda de dados e consequentemente informação de negócio.

A decisão sobre o valor do RPO é o elemento singular de maior importância, a ser tomado pelos donos de cada recurso da organização.

1 Nota do autor: as ações autoexplicativo estão suprimidas.

P

APÊNDICE P — PROVIDENCIAR E UTILIZAR UM GESTOR DE SEGREDOS

É de suma importância a utilização de um gestor de segredos, pela contribuição na proteção de dados sensíveis. Garante-se assim, palavras-passe complexas, longas e únicas e, em caso de comprometimento de um dos segredos, os restantes continuam salvaguardados.

Entregáveis[1]:

- *Existir um programa de gestão de segredos aprovado para uso na organização e fornecido a todos os utilizadores*: um bom programa de gestão de segredos deve providenciar as funcionalidades de:
  - Encriptação através da cifra AES 256-BIT;
  - Autenticação MFA;
  - Incluir um gerador de senhas;
  - Identificar senhas fracas e duplicadas;
  - Permitir partilha segura de segredos com terceiros;
  - Permissões individualizadas e de grupo;
  - Compatibilidade com múltiplos SO;
  - Registo das ações dos utilizadores para posterior auditoria.

  Dependendo dos objetivos, capacidade financeira e cenários em causa, as opções ulteriores são uma escolha válida:
  - *Bitwarden*[2];
  - *KeePass*[3].
- *Consciencializar todos os utilizadores para a importância e obrigatoriedade do seu uso*: verificar o apêndice J.

1 Nota do autor: as ações autoexplicativo estão suprimidas.
2 https://bitwarden.com/
3 https://keepass.info/

- *Impor a obrigatoriedade de MFA no acesso à ferramenta*: ver o apêndice I.

APÊNDICE Q — CONFIGURAÇÃO DE REGISTOS E ALERTAS

O registo de eventos permite identificar potenciais causas de erros e falhas, que ocorrem nos sistemas. Por outro lado, através da monitorização e análise dos *logs*, a deteção e resposta a ameaças de segurança torna-se mais eficaz e diminui-se o risco de ocorrência de violações de informação. Sem esquecer da obrigatoriedade de manter registos por parte de múltiplas regulações, normativos e legislação, sendo fonte de evidência em auditorias e disputas legais.

Entregáveis[1]:

- *Enviar os registos para um sistema de armazenamento e análise centralizado*: a escolha de um sistema de análise e correlação de registos deve englobar as funcionalidades:
  - Recolha de *logs* de múltiplas fontes, como *firewalls*, servidores, subscrições na nuvem, base de dados;
  - Correlação de eventos das várias fontes na identificação de padrões e incidentes de segurança da informação;
  - Monitorização em tempo real;
  - Integração de *threat intelligence feeds*;
  - Geração de relatórios e personalização de *dashboards*;
  - Integração com outras ferramentas de segurança, como, sistemas de gestão de incidentes e deteção de vulnerabilidades.

  Duas escolhas acertadas como solução SIEM:

  - *Graylog*[2]: gestão centralizada de registos, pesquisa em tempo real e integração com várias fontes de dados, como *Syslog*, GELF e SNMP;

1 Nota do autor: as ações autoexplicativo estão suprimidas.
2 https://www.graylog.org/

  - *Security Onion*[3]: inclui captura de pacotes de rede, análise e deteção de intrusão, e uma panóplia de ferramentas de segurança poderosas, como o *Snort*, *Suricata* e *Zeek*.

- *Os registos devem ser alvo de cópia de segurança e guardados, no mínimo, um ano; alguns tipos de informação podem ter de ser retidos por um período não inferior a seis anos (e.g., registos clínicos de pacientes)*: face à introdução do RGPD, os dados de índole pessoal devem ser conservados durante o mínimo de tempo possível, tendo em consideração as finalidades para as quais são tratados. Um valor comummente aceite para os registos informáticos é noventa dias.
- Tipificação de *logs* que as organizações devem considerar a monitorizar:
  - Registos de Autenticação: tentativas de início de sessão do utilizador com sucesso e insucesso;
  - Registos de Autorização: acessos a ficheiros, utilização de aplicações e atividades (e.g., criar, apagar, modificar, eliminar) padrão e privilegiadas dos utilizadores;
  - Registos de Sistema: eventos, erros e alarmes;
  - Registos de Aplicação: atividades e erros;
  - Registos de *Firewall*: ligações permitidas e proibidas;
  - Registos de Antivírus: deteção de *malware*, quarentena e ações de limpeza;
  - Registos de Servidores *Web*: pedidos, respostas e acessos efetuados aos servidores;
  - Registos de *Email*: detalhes do remetente, destinatário, assunto e anexos.

3 https://github.com/Security-Onion-Solutions/securityonion/blob/master/VERIFY_ISO.md

R

APÊNDICE R — CICLO DE VIDA DOS ATIVOS

Os ativos são o elemento primordial na identificação de riscos, ou seja, para cada ativo há um leque de ameaças e vulnerabilidades, que devem ser consideradas e controlos implementados, por forma a garantir o seu tratamento adequado. Por outro lado, é fundamental a determinação do dono de cada ativo, para garantir a responsabilidade (*accountability*) e a proteção da informação armazenada, transmitida ou processada pelo mesmo.

Não menos importante é a capacidade da organização, ao ter uma visão holística de todos os ativos, poder endereçar falhas nos dados, elementos redundantes ou desatualizados, consolidar diferentes fontes de informação e identificar inconsistências, que permitam melhor a qualidade dos dados nos ativos.

Um ativo é tudo o que tenha valor para uma determinada entidade. Importa, portanto, não somente colocar o foco no *hardware* e *software*, mas também, alargar o âmbito a todos os ativos de informação que possam armazenar, transportar e processar dados. Uma pessoa pode ser um ativo (visto as pessoas poderem armazenar informação como conhecimento, transportar informação pela comunicação, ou processar informação através do raciocínio), um objeto (e.g., um pedaço de papel), ou uma tecnologia (e.g., uma base de dados).

Na Figura 48 podemos encontrar um leque de atributos, considerados relevantes pelo autor, que devem fazer parte das propriedades de cada ativo. Obviamente, dependendo da especificidade do tipo de ativo em causa, há, por certo, campos não aplicáveis e outros a considerar.

Atributo	Descrição
Administrador do ativo	Executor das operações técnicas (e.g, intervenções de manutenção).
Ambiente	e.g., produção, qualidade, desenvolvimento.
Data de Validação	Data da última validação pelo dono do ativo da qualidade dos dados.
Descrição	Descrição do ativo.
Dono (*owner*) do ativo	Responsável de negócio.
Estado	e.g., produção, retirado, rascunho.
FQDN	*Fully qualified domain name.*
Gestor do ativo	Responsável pelas operações diárias.
IP	*Internet protocol.*
Localização	e.g., região, país.
Nível de segurança	Representa o nível de segurança, i.e., os requisitos, a que o ativo está sujeito. Por exemplo, uma aplicação que contenha registos com informação sensível terá um nível superior a uma outra que albergue informação somente de caracter público.
Nome	Nome do ativo.
Responsável de segurança	e.g., ISO, CISO.
Tipo de ativo	e.g., servidor, impressora, base de dados.
Visibilidade	e.g., *internet*, *intranet*.

Figura 48: Atributos do Ativo

Entregáveis[1]:

- *Registar todos os ativos de sistema, incluindo software e hardware*: o registo pode ser efetuado em qualquer suporte (e.g., folha de cálculo), no entanto, a utilização de um programa para o efeito otimiza o processo (e.g., pesquisa) e diminui os erros e falhas. Os seguintes são recomendáveis:
  - *Lansweeper*[2];
  - *Snipe-IT*[3];
  - *GLPI*[4];
  - *Open-AudIT*[5].
- *Todos os ativos são objeto de parametrizações de robustez antes de serem utilizados, sendo mantidos regularmente com atualizações e correções*: observar o apêndice F.
- *Os ativos desativados são removidos do meio envolvente e destruídos em segurança*: todos os suportes de armazenamento (e.g., discos rígidos, impressoras, *firewalls*, embebidos em *appliances*, papel, discos óticos) devem ser objeto de um processo de eliminação. A organização deve adotar um dos métodos seguintes:
  - Encriptação do arquivo de armazenamento.

1 Nota do autor: as ações autoexplicativo estão suprimidas.
2 https://www.lansweeper.com/
3 https://snipeitapp.com/
4 https://glpi-project.org/
5 https://www.open-audit.org/

  - Incineração, retalho, fragmentação do dispositivo físico.
  - Programa que implemente o padrão de eliminação e sanitização do DOD 5220.22-M, como no caso do:
    * *SDelete*[6];
    * *Scrub*[7].

- *Classificar o quão crítico cada tipo de informação é, para as operações contínuas do negócio e definir uma classificação geral ou pontuação de risco*: analisar o apêndice V.
- *Determinar o impacto global potencial da informação*: verificar o apêndice V.

6 https://learn.microsoft.com/en-us/sysinternals/downloads/sdelete
7 https://github.com/chaos/scrub

S

APÊNDICE S — APLICAR O PRINCÍPIO DO MENOR PRIVILÉGIO

Princípio fundamental de segurança da informação, no qual se advoga a atribuição do nível mínimo de acesso necessário, à execução da função a desempenhar. Minimiza o risco de acesso não autorizado, reduz o dano potencial ou a exfiltração de dados, reforça a responsabilidade individual e assegura conformidade com aspetos legais e regulatórios (e.g., RGPD).

Entregáveis[1]:

- *Perceber o nível mínimo de permissões necessárias, para todos os utilizadores na organização*: uma matriz de acessos por função, é aconselhável ser criada para as contas de utilizadores, segundo os requisitos definidos pelo dono de cada ativo. As contas de sistema e serviço, também carecem de registo por recurso (e.g., aplicação, servidor, partilha de ficheiros, subscrição na nuvem):

Tabela 81: Matriz de Acessos

Função	**Recurso 1**	**Recurso 2**	**...**	**Recurso N**
Contabilista	Leitura	Escrita	...	Total
Operador Fabril	Não Aplicável	Não Aplicável	...	Não Aplicável
...	...	...	...	...

  Assim, no processo de admissão/demissão/mudança de funções de um colaborador, o ajuste de permissões, quer realizado automaticamente ou manualmente, torna-se mais eficiente.

- *Rever os acessos dos utilizadores para garantir, que mantêm o menor nível de permissões necessárias para o seu trabalho*: o dono de cada ativo, precisa de rever os utilizadores e respetivos acessos ciclicamente, pelo menos anualmente.

- *Atribuir contas separadas a utilizadores que necessitem de permissões administrativas ou sensíveis. Uma conta tem as permissões administrativas, e a outra tem permissões menores para outros aspetos do seu trabalho*: qualquer conta adicional atribuída a um utilizador deve-o identificar, além de especificar a funcionalidade assegurada. Por exemplo `<nome-de-utilizador_admin>`.

1 Nota do autor: as ações autoexplicativo estão suprimidas.

- *Registar as ações tomadas pelos utilizadores administrativos e enviar os eventos para um repositório central para análise e alerta. Configurar regras de envio de notificações, quando ações inesperadas acontecem, tais como, alterações durante horas invulgares do dia.*: constatar o apêndice Q.
- *Requerer palavras-passe fortes e únicas para cada conta.* observar o apêndice I.

APÊNDICE T — IMPLEMENTAR SEGMENTAÇÃO DE REDE

A divisão dos ativos de rede em diferentes segmentos, melhora a gestão, segurança e o desempenho. Redes segmentadas simplificam as tarefas de manutenção e resolução de problemas. Por outro lado, contribuem para o isolamento de ameaças de segurança e dificultam a movimentação lateral por parte de atores maliciosos.

Entregáveis[1]:

- *Todos os dispositivos sensíveis, estão separados de outros sistemas mantidos em redes segmentadas*: utilizar um ou mais dos seguintes métodos:
  - VLAN: agrupar ativos em redes lógicas, baseados na sua função, tipo ou localização;
  - *Subnets*: separação suportada em endereços IP;
  - *Firewalls*: restrição de acessos entre segmentos pela restrição de tráfego, baseado em protocolos, portos e endereços IP;
  - NAC: controlo da rede através da utilização de políticas, que restringem o acesso à rede dependendo do tipo de dispositivo, entre outros fatores;
  - SDN: utilização de *sofware* em vez de *hardware*, para ajustar dinamicamente os segmentos de rede, com base em condições como volume de tráfego ou ameaças de segurança;
  - *Zero Trust*: aplicação do princípio de verificação e limitação em cada acesso por parte do utilizador e dispositivo específico, a dados e aplicações.
- *Todos os dispositivos da rede são robustecidos e mantidos*: onservar o apêndice F.
- *Os eventos são registados e armazenados num local central, para capturar alterações de segurança e de configuração de autenticação nos dispositivos de rede e nas suas regras, tráfego de rede suspeito e tentativas de autenticação*: conferir o apêndice Q.

1 Nota do autor: as ações autoexplicativo estão suprimidas.

APÊNDICE U — IMPLEMENTAR PROCESSOS DE VERIFICAÇÃO

Os processos de verificação são basilares na contribuição para uma eficaz, segura e conforme proteção dos ativos corporativos, garantindo maior confiança das partes interessadas na condução de atividades económicas na e com a organização.

Entregáveis[1]:

- *Elaborar um processo, seguido pelos utilizadores, para verificar todos os pedidos num canal de comunicação separado, antes de serem executados*:
  - Averiguar a identidade da terceira parte, e.g., documento de identificação, endereço de correio eletrónico, número de telefone, biometria;
  - Usar *software* de deteção de fraude, i.e., analisar padrões anómalos nas transações;
  - Monitorizar as transações em tempo real, na tentativa de detetar mais rapidamente atividade suspeita e terminar uma transação fraudulenta antes de ser completada;
  - Implementar limite máximo de pagamento numa única transação;
  - Educar os colaboradores acerca de prevenção e deteção de fraudes nos pagamentos;
  - Manter o *software* e *hardware* que processa os pagamentos atualizado;
  - Usar unicamente métodos de pagamento seguros, e.g., *gateways* de pagamento.
- *Relatar e registar todos os eventos de segurança e pedidos não autorizados como parte do processo de gestão de incidentes de segurança da sua organização*: analisar o apêndice X.
- *Fazer uma verificação completa, nacionalmente, dos antecedentes criminais, infrações sexuais e, se possível, responsabilidades de crédito, de todos os potenciais empregados (especialmente se vão manusear fundos empresariais);*

1 Nota do autor: as ações autoexplicativo estão suprimidas.

escolas frequentadas, grau académico, data de graduação, média académica e referências: incluir nas verificações de antecedentes os pontos ulteriores:

- Identidade da pessoa;
- Veracidade da morada;
- Pesquisa em motores de busca;
- Análise de plausibilidade do CV;
- Pedido do registo criminal;
- Avaliação de crédito;
- Existência de conflito de interesses;
- Historial da relação laboral com as entidades anteriores;
- Averiguação da educação, incluindo cursos e certificados.

V

APÊNDICE V — COMPREENDER AS AMEAÇAS E VULNERABILIDADES DO NEGÓCIO

A compreensão das ameaças e vulnerabilidades é crucial ao negócio, de modo a se desenvolverem estratégias efetivas de mitigação e gestão do risco. Somente a condução de uma avaliação de risco, permite a identificação de potenciais ameaças, a consideração dos impactos e estimativas das *likelihoods* e o desenvolvimento de táticas de limitação de danos e efeitos negativos. A concretização destas tarefas, permite o estabelecimento de medidas robustas de cibersegurança, a implementação de protocolos físicos seguros, a manutenção de práticas financeiras credíveis e a priorização da conformidade face a relevantes regulações e normativos de mercado.

Entregáveis[1]:

- *Identificar estratégias específicas de proteção contra ameaças ou vulnerabilidades, através da revisão regular das ameaças e vulnerabilidades, que podem afetar o negócio e estimar a likelihood de afetação dessa ameaça ou vulnerabilidade*: normativos como o PCI DSS descrevem, requisito 12.1.2 (PCI, 2012), a necessidade de se incluir um processo anual, que identifique ameaças, vulnerabilidades e resulte numa avaliação de risco formal. Indica também algumas metodologias que podem ser seguidas, como a OCTAVE[2], ISO/IEC 27005[3] e NIST SP 800-30[4].
  O autor propõe uma abordagem assente na Identificação, Classificação e Proteção do Ativo (ICPA).

v.0.1 *Identificação, Classificação e Proteção do Ativo*

O processo ICPA consiste em seis fases:

1 Nota do autor: as ações autoexplicativo estão suprimidas.
2 https://resources.sei.cmu.edu/asset_files/TechnicalReport/1999_005_001_16769.pdf
3 https://www.iso.org/standard/80585.html
4 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

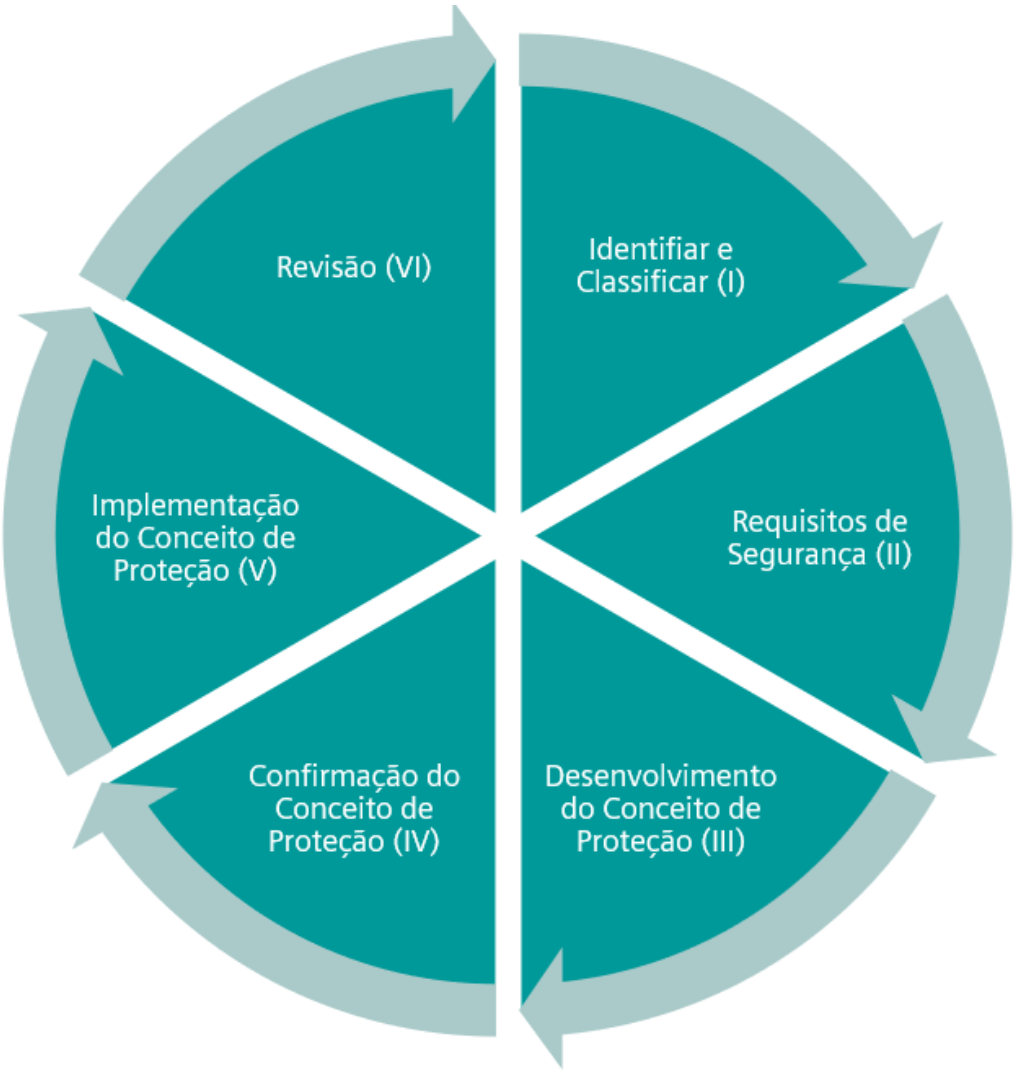


Figura 49: Processo ICPA

Identificar e Classificar (I): nesta fase todos os ativos são identificados e classificados em termos da sua criticidade para o negócio em cada dimensão CIA, consoante o estabelecido no BIA, conforme descrito na subsecção V.0.2. O Dono do Ativo classifica o recurso em causa, podendo se socorrer de especialistas (e.g., DPO, CISO), durante o processo. O entregável desta fase é o nível ICPA do ativo para cada dimensão CIA.

Requisitos de Segurança (II): tendo o nível ICPA do ativo definido, são reunidas a série de ações correspondentes do Portfólio de Controlos 4.2. O entregável desta fase são o conjunto de *Regras* (ações) específicas para o ativo em causa.

Desenvolvimento do Conceito de Proteção (III): consiste no questionário baseado no conjunto de *Regras*. Na resposta a cada ação (questão) é avaliada se cumpre ou não o descrito. Se cumprir é considerada em conformidade. Se não

cumprir, há um desvio à *Regra* em causa. Em ambos os casos é atribuído um nível de risco V.0.3. O questionário é preenchido pelo Gestor do Ativo. Especialistas (e.g., jurísta, administrador de sistemas) podem ajudar no preenchimento. A análise de risco é efetuada pelo CISO ou um deputado. Assim se garante o *Four Eyes Principle*. O CISO percorre a lista de todos os desvios às *Regras*, indicando o nível de risco para cada desvio, negociando com o Gestor do Ativo, a sua mitigação ou aceitação. No caso da opção de mitigação, também é indicado a resolução, quantificação do custo financeiro não operacional, responsável pela mitigação e data de conclusão da tarefa. O entregável desta fase é a análise de risco do ativo, tendo por base as *Regras* de segurança e privacidade da informação estabelecidas na organização.

Confirmação do Conceito de Proteção (IV): a confirmação do Conceito de Proteção é efetuado pelo Dono do Ativo e é sua responsabilidade dar anuência a cada risco proveniente da etapa precedente. Nesta fase, é sempre possível ajustar a análise de risco, alterando o estado de um risco de mitigação para aceitação ou vice-versa. O entregável desta fase é a lista de desvios (riscos) às *Regras* confirmada.

Implementação do Conceito de Proteção (V): implementação dos elementos da lista de desvios às *Regras* aprovadas no ponto antecedente. O responsável pela implementação de cada medida, quando a soluciona, submete o descritivo e evidência da resolução, sendo aprovada ou não, pelo CISO. Se aprovada fica concluída. Se não aprovada, é reaberta a atividade, sendo explanado os passos suplementares que continuam em falta. O entregável desta fase é o ativo protegido segundo os requisitos de segurança da informação em vigor na organização.

Revisão (VI): O processo é reavaliado e confirmado anualmente ou quando existe uma alteração significativa.

Com este método, obtém-se uma enorme consistência e normalização da análise e tratamento dos riscos, envolvendo as diversas partes interessadas do ativo. Aplica-se a cada ativo (objeto) e não há classe do ativo, praticando-se o mesmo conjunto de *Regras*, uniformemente, resultando num nível de confiança na proteção do ativo cabal.

v.0.2 Business Impact Analysis

Adaptar os **critérios** e **valores** à natureza e objeto social da organização

A tabela é executada para cada uma das dimensões CIA

Escala	1	3	5	7	9
Critérios	**Irrelevante**	**Diminuto**	**Limitado**	**Apreciável**	**Severo**
Partes interessadas afetadas	< 10	>=10 e <50	>=50 e <100	>=100 e <200	>=200
Impacto económico e financeiro	<1000€ em custos diretos e indiretos	>=1000€ e <2500€ em custos diretos e indiretos	>= 2500€ <5000€ em custos diretos e indiretos	>= 5000€ e < 10000€ em custos diretos e indiretos	>=10000€ em custos diretos e indiretos
Impacto na reputação	Sem cobertura mediática	Cobertura em meio de comunicação local	Cobertura em meio de comunicação local e comunicado à imprensa nacional	Cobertura mediática nacional e redes sociais	Cobertura mediática nacional, internacional e redes sociais
Ativação de planos de contingência	Sem ativação de qualquer plano	Ativação de plano de contingência em localização secundária	Ativação de múltiplos planos de contingência em localização secundária	Ativação de múltiplos planos de contingência em localização principal	Ativação de múltiplos planos de contingência em localização principal e secundária
Intervenção da gestão de topo	Sem intervenção da gestão de topo	Intervenção esporádica da gestão de topo circunscrita a minúcias	Intervenção não continuada da gestão de topo durante o período de ocorrência ou resolução	Acompanhamento da gestão de topo numa base continuada durante o período de ocorrência ou resolução	Acompanhamento da gestão de topo numa base continuada durante o período de ocorrência e resolução
Incumprimentos legais ou regulamentares	Sem incumprimentos	Incumprimentos menores	Incumprimentos moderados	Falha ou risco de litígio nas obrigações legais ou contratuais com terceiros	Falha ou risco de litígio sistémico nas obrigações legais ou contratuais com terceiros
Notificação formal a autoridades competentes a nível nacional ou internacional	Sem notificação	Consulta informal a uma autoridade competente local ao país da ocorrência do facto	Consulta informal a múltiplas autoridades competentes locais ao país da ocorrência do facto	Notificação formal a uma ou mais autoridades nacionais (e.g., CNPD, PJ)	Notificação formal a uma ou mais autoridades nacionais e internacionais (e.g., ENISA, Europol)
Avaliação de especialistas	De acordo com a avaliação dos especialistas	De acordo com a avaliação dos especialistas (e.g., CISO, DPO)	De acordo com a avaliação dos especialistas (e.g., CISO, DPO)	De acordo com a avaliação dos especialistas (e.g., CISO, DPO)	De acordo com a avaliação dos especialistas (e.g., CISO, DPO)
Objetivos de negócio	Sem impacto	Impacto nos objetivos de curto prazo	Impacto nos objetivos de médio prazo	Impacto num dos objetivos de longo prazo	Impacto em múltiplos objetivos de longo prazo da organização
ICPA	**Nível / Perfil Nuclear**			**Nível / Perfil Definido**	**Nível / Perfil Otimizado**

Figura 50: Matriz BIA

v.0.3 *Nível de Risco*

LIKELIHOOD	1	2	3	4	5
IMPACTO	Nunca ocorreu na organização	Já ouvi falar, mas nunca ocorreu na organização	Já ocorreu num passado distante na organização	Já ocorreu num passado recente na organização	Já ocorreu num passado recente na organização mais do que uma vez
Severo 9	18	27	36	45	54
Apreciável 7	14	21	28	35	42
Limitado 5	10	15	20	25	30
Diminuto 3	6	9	12	15	18
Irrelevante 1	2	3	4	5	6
Nível de risco	= Impacto + (Impacto * (*Likelihood sem contra medidas – controlos aplicados*))				

Figura 51: Cálculo do Nível de Risco

Primeiro: o vetor **Impacto** estima-se com base no BIA. Em cada dimensão aplicável, verifica-se qual é o critério ou critérios com o maior número entre 1 e 9, sendo esse valor o atribuído à respetiva dimensão. A seguir obtêm-se o máximo valor entre as dimensões, sendo essa a grandeza do impacto.

Segundo: o vetor ***Likelihood*** afere-se com base nos eventos ocorridos de tentativa e facilidade na exploração da fraqueza, após se ter tido em consideração os controlos em vigor.

Terceiro: O **Nível de Risco** é calculado aplicando a fórmula:

```
Função(Impacto, Likelihood, Controlo Aplicados)= Impacto + (Impacto
* (Likelihood sem contra medidas - controlos aplicados))
```

O intuito da função é enfatizar a componente de negócio, tanto pelo peso da quantificação acrescida, bem como a adição duplicada do vetor impacto, em detrimento da *likelihood*.
O tratamento segue o descrito na figura sequente:

Nível de Risco	
	O risco necessita de ser tratado, no espaço temporal de 90 dias, ou ser aceite pelo dono do ativo e pela gestão de topo.
	O risco necessita de ser tratado, no espaço temporal de 180 dias, ou ser aceite pelo dono do ativo.
	O risco necessita de ser tratado, no espaço temporal de 365 dias, ou ser aceite pelo gestor do ativo.

Figura 52: Tratamento do Nível de Risco

v.0.4 *Ensaio ICPA*

Demonstração simplificada do processo ICPA sobre o ativo: aplicação ERP da organização.

I: o Dono do Ativo é o gestor financeiro, que classifica o ativo em cada uma das dimensões. O resultado é demonstrado nas tabelas seguintes:

Escala	1	3	5	7	9
Critérios	**Irrelevante**	**Diminuto**	**Limitado**	**Apreciável**	**Severo**
Partes interessadas afetadas	< 10	>=10 e <50	>=50 e <100	>=100 e <200	>=200
Impacto económico e financeiro	<1000€ em custos diretos e indiretos	>=1000€ e <2500€ em custos diretos e indiretos	>= 2500€ <5000€ em custos diretos e indiretos	>= 5000€ e < 10000€ em custos diretos e indiretos	>=10000€ em custos diretos e indiretos
Impacto na reputação	Sem cobertura mediática	Cobertura em meio de comunicação local	Cobertura em meio de comunicação local e comunicado à imprensa nacional	Cobertura mediática nacional e redes sociais	Cobertura mediática nacional, internacional e redes sociais
Ativação de planos de contingência	Sem ativação de qualquer plano	Ativação de plano de contingência em localização secundária	Ativação de múltiplos planos de contingência em localização secundária	Ativação de múltiplos planos de contingência em localização principal	Ativação de múltiplos planos de contingência em localização principal e secundária
Intervenção da gestão de topo	Sem intervenção da gestão de topo	Intervenção esporádica da gestão de topo circunscrita a minúcias	Intervenção não continuada da gestão de topo durante o período de ocorrência ou resolução	Acompanhamento da gestão de topo numa base continuada durante o período de ocorrência ou resolução	Acompanhamento da gestão de topo numa base continuada durante o período de ocorrência e resolução
Incumprimentos legais ou regulamentares	Sem incumprimentos	Incumprimentos menores	Incumprimentos moderados	Falha ou risco de litígio nas obrigações legais ou contratuais com terceiros	Falha ou risco de litígio sistémico nas obrigações legais ou contratuais com terceiros
Notificação formal a autoridades competentes a nível nacional ou internacional	Sem notificação	Consulta informal a uma autoridade competente local ao país da ocorrência do facto	Consulta informal a múltiplas autoridades competentes locais ao país da ocorrência do facto	Notificação formal a uma ou mais autoridades nacionais (e.g., CNPD, PJ)	Notificação formal a uma ou mais autoridades nacionais e internacionais (e.g., ENISA, Europol)
Avaliação de especialistas	De acordo com a avaliação dos especialistas	De acordo com a avaliação dos especialistas (e.g., CISO, DPO)	De acordo com a avaliação dos especialistas (e.g., CISO, DPO)	De acordo com a avaliação dos especialistas (e.g., CISO, DPO)	De acordo com a avaliação dos especialistas (e.g., CISO, DPO)
Objetivos de negócio	Sem impacto	Impacto nos objetivos de curto prazo	Impacto nos objetivos de médio prazo	Impacto num dos objetivos de longo prazo	Impacto em múltiplos objetivos de longo prazo da organização
ICPA	**Nível / Perfil Nuclear**			**Nível / Perfil Definido**	**Nível / Perfil Otimizado**

Figura 53: Dimensão Confidencialidade

Escala	1	3	5	7	9
Critérios	**Irrelevante**	**Diminuto**	**Limitado**	**Apreciável**	**Severo**
Partes interessadas afetadas	< 10	>=10 e <50	>=50 e <100	>=100 e <200	>=200
Impacto económico e financeiro	<1000€ em custos diretos e indiretos	>=1000€ e <2500€ em custos diretos e indiretos	>= 2500€ <5000€ em custos diretos e indiretos	>= 5000€ e < 10000€ em custos diretos e indiretos	>=10000€ em custos diretos e indiretos
Impacto na reputação	Sem cobertura mediática	Cobertura em meio de comunicação local	Cobertura em meio de comunicação local e comunicado à imprensa nacional	Cobertura mediática nacional e redes sociais	Cobertura mediática nacional, internacional e redes sociais
Ativação de planos de contingência	Sem ativação de qualquer plano	Ativação de plano de contingência em localização secundária	Ativação de múltiplos planos de contingência em localização secundária	Ativação de múltiplos planos de contingência em localização principal	Ativação de múltiplos planos de contingência em localização principal e secundária
Intervenção da gestão de topo	Sem intervenção da gestão de topo	Intervenção esporádica da gestão de topo circunscrita a minúcias	Intervenção não continuada da gestão de topo durante o período de ocorrência ou resolução	Acompanhamento da gestão de topo numa base continuada durante o período de ocorrência ou resolução	Acompanhamento da gestão de topo numa base continuada durante o período de ocorrência e resolução
Incumprimentos legais ou regulamentares	Sem incumprimentos	Incumprimentos menores	Incumprimentos moderados	Falha ou risco de litígio nas obrigações legais ou contratuais com terceiros	Falha ou risco de litígio sistémico nas obrigações legais ou contratuais com terceiros
Notificação formal a autoridades competentes a nível nacional ou internacional	Sem notificação	Consulta informal a uma autoridade competente local ao país da ocorrência do facto	Consulta informal a múltiplas autoridades competentes locais ao país da ocorrência do facto	Notificação formal a uma ou mais autoridades nacionais (e.g., CNPD, PJ)	Notificação formal a uma ou mais autoridades nacionais e internacionais (e.g., ENISA, Europol)
Avaliação de especialistas	De acordo com a avaliação dos especialistas	De acordo com a avaliação dos especialistas (e.g., CISO, DPO)	De acordo com a avaliação dos especialistas (e.g., CISO, DPO)	De acordo com a avaliação dos especialistas (e.g., CISO, DPO)	De acordo com a avaliação dos especialistas (e.g., CISO, DPO)
Objetivos de negócio	Sem impacto	Impacto nos objetivos de curto prazo	Impacto nos objetivos de médio prazo	Impacto num dos objetivos de longo prazo	Impacto em múltiplos objetivos de longo prazo da organização
ICPA	**Nível / Perfil Nuclear**			**Nível / Perfil Definido**	**Nível / Perfil Otimizado**

Figura 54: Dimensão Integridade

Escala	1	3	5	7	9
Critérios	**Irrelevante**	**Diminuto**	**Limitado**	**Apreciável**	**Severo**
Partes interessadas afetadas	< 10	>=10 e <50	>=50 e <100	>=100 e <200	>=200
Impacto económico e financeiro	<1000€ em custos diretos e indiretos	>=1000€ e <2500€ em custos diretos e indiretos	>= 2500€ <5000€ em custos diretos e indiretos	>= 5000€ e < 10000€ em custos diretos e indiretos	>=10000€ em custos diretos e indiretos
Impacto na reputação	Sem cobertura mediática	Cobertura em meio de comunicação local	Cobertura em meio de comunicação local e comunicado à imprensa nacional	Cobertura mediática nacional e redes sociais	Cobertura mediática nacional, internacional e redes sociais
Ativação de planos de contingência	Sem ativação de qualquer plano	Ativação de plano de contingência em localização secundária	Ativação de múltiplos planos de contingência em localização secundária	Ativação de múltiplos planos de contingência em localização principal	Ativação de múltiplos planos de contingência em localização principal e secundária
Intervenção da gestão de topo	Sem intervenção da gestão de topo	Intervenção esporádica da gestão de topo circunscrita a minúcias	Intervenção não continuada da gestão de topo durante o período de ocorrência ou resolução	Acompanhamento da gestão de topo numa base continuada durante o período de ocorrência ou resolução	Acompanhamento da gestão de topo numa base continuada durante o período de ocorrência e resolução
Incumprimentos legais ou regulamentares	Sem incumprimentos	Incumprimentos menores	Incumprimentos moderados	Falha ou risco de litígio nas obrigações legais ou contratuais com terceiros	Falha ou risco de litígio sistémico nas obrigações legais ou contratuais com terceiros
Notificação formal a autoridades competentes a nível nacional ou internacional	Sem notificação	Consulta informal a uma autoridade competente local ao país da ocorrência do facto	Consulta informal a múltiplas autoridades competentes locais ao país da ocorrência do facto	Notificação formal a uma ou mais autoridades nacionais (e.g., CNPD, PJ)	Notificação formal a uma ou mais autoridades nacionais e internacionais (e.g., ENISA, Europol)
Avaliação de especialistas	De acordo com a avaliação dos especialistas	De acordo com a avaliação dos especialistas (e.g., CISO, DPO)	De acordo com a avaliação dos especialistas (e.g., CISO, DPO)	De acordo com a avaliação dos especialistas (e.g., CISO, DPO)	De acordo com a avaliação dos especialistas (e.g., CISO, DPO)
Objetivos de negócio	Sem impacto	Impacto nos objetivos de curto prazo	Impacto nos objetivos de médio prazo	Impacto num dos objetivos de longo prazo	Impacto em múltiplos objetivos de longo prazo da organização
ICPA	**Nível / Perfil Nuclear**			**Nível / Perfil Definido**	**Nível / Perfil Otimizado**

Figura 55: Dimensão Disponibilidade

O valor máximo de cada dimensão é CIA (BIA) = 997. O valor IPCA = Otimizado, Otimizado, Definido. Conclui-se que em termos de impacto para o negócio, o ativo aplicação ERP é de nível Otimizado.

II: a partir do ICPA e tipo de ativo, filtra-se as *Regras* a cumprir a partir do Portfólio de Controlos.

III: criação do Conceito de Proteção. Ilustra-se dois requisitos para este tipo de ativo:

Identificador	Questão	Resposta	Impacto Máximo	*Likelihood* s/ Controlos	*Likelihood Atual*	*Likelihood* c/ Controlos
1.13.47	Testar as cópias de segurança periodicamente?	Testes aleatórios sem um plano anual definido.	7 (A)	3	2	1
1.30.60	Conduzir uma análise ou varredura de vulnerabilidades por um profissional, pelo menos anualmente, e sempre que haja alterações substanciais nos computadores e rede?	Existe um programa de vulnerabilidades com execução semanal sobre o ativo ERP.	9 (CIA)	4	1	1
(...)	(...)	(...)	(...)		(...)	(...)

Figura 56: Amostra do Conceito de Proteção

Enquanto o risco proveniente do identificador 1.30.60 encontra-se no nível residual mínimo, para o identificador 1.13.47 é necessário a implementação de mitigações adicionais.

Acordou-se com o Gestor do Ativo, o contabilista, a implementação de um plano de testes trimestral, no prazo de até 60 dias.

IV: o Dono do Ativo concordou com a elaboração do Conceito de Proteção, tendo sido confirmado.

V: A medida foi submetida no prazo acordado e a mitigação avaliada e evidenciada pelo CISO favoravelmente. Como nota, caso o prazo não seja cumprido, é iniciado um fluxo de notificações para o Dono do Ativo entre outras partes interessadas.

VI: o processo é reiniciado após um ano.

APÊNDICE W — CRIAR POLÍTICAS E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

As políticas contribuem para o estabelecer de expetativas no ambiente corporativo, assegurar a conformidade, mitigar riscos, promover a responsabilização, mas sobretudo servem para colmatar a ineficácia dos controlos técnicos.

Entregáveis[1]:

- *As políticas e procedimentos de segurança da informação e cibersegurança, devem descrever as expectativas para proteger as informações e sistemas; identificar os recursos e informações importantes; a perspetiva da gestão relativamente ao uso e proteção dos recursos por parte dos colaboradores; e enumerar as práticas aceitáveis e expectativas para as operações de negócio*: a primeira e mais importante política a ser definida e da qual derivam as restantes é a Política de Segurança e Privacidade da Informação. O objetivo é a definição das diretivas para a organização e a proteção dos seus ativos de informação contra todas as ameaças internas, externas, deliberadas ou acidentais.
  O texto ulterior apresenta a definição completa de tal política.

  Política de Segurança e Privacidade da Informação

  - O objetivo da Gestão de Segurança e Privacidade da Informação na *nome_da_organização* é garantir a proteção dos seus ativos de informação, a continuidade do seu negócio e a mitigação dos seus riscos, prevenindo os incidentes de segurança e privacidade da informação e reduzindo o seu potencial impacto.
  - A estratégia de segurança e privacidade delineada pela gestão de topo passa por considerar a informação como um ativo de negócio, um risco de informação como uma questão de negócio, a segurança e privacidade da informação como uma estrutura que suporta o negócio em alcançar os seus objetivos, e consequentemente, o Sistema de Gestão de Segurança e

1 Nota do autor: as ações autoexplicativo estão suprimidas.

Privacidade da Informação é um alicerce de governação que capacita o negócio.

- A gestão de topo está empenhada e comprometida em assegurar e garantir a conformidade e responsabilidades com toda a legislação e regulamentação relacionada com a proteção de Dados Pessoais e termos contratuais acordados entre a *nome_da_organização* e os seus parceiros, subcontratados e restantes terceiras partes (e.g., clientes, fornecedores).
- A Política de Segurança e Privacidade da Informação garante que:
  - Os ativos de informação são protegidos contra todos os acessos não autorizados;
  - A confidencialidade da informação é preservada;
  - A integridade e disponibilidade da informação são mantidas;
  - A resiliência permanente dos sistemas e dos serviços de tratamento de informação são garantidos;
  - Os requisitos legais, legislativos, regulamentares, estatutários, normativos e contratuais são cumpridos;
  - Os Planos de Continuidade de Negócio são definidos, mantidos e testados;
  - A informação é classificada de acordo com a sua importância para a organização e requisitos legais;
  - Os objetivos de segurança e privacidade da informação são estabelecidos por forma a proteger a Confidencialidade, Integridade e Disponibilidade dos ativos de informação identificados tendo em consideração o contexto da organização e o inventário de ativos;
  - As responsabilidades e funções no SGPI são atribuídas pela gestão de topo por forma a assegurar conformidade com os requisitos;
  - A formação em segurança e privacidade de informação é disponibilizada a todos os colaboradores;
  - Todos os incidentes relacionados com a segurança e privacidade de informação são reportados e adequadamente investigados;
  - Todas as equipas estão comprometidas com, e colaboraram ativamente para o cumprimento da Política de Segurança e Privaci-

dade da Informação e melhoria contínua do Sistema de Gestão da *nome_da_organização*;

  * Os Dados Pessoais são objeto de um tratamento lícito, leal e transparente em relação ao Titular dos Dados e são recolhidos para finalidades determinadas, explícitas e legítimas não sendo tratados de uma forma incompatível com essas finalidades;

  * No desenvolvimento e manutenção de políticas de segurança da informação, é considerada a legislação e regulamentação específica que incida sobre o processo de tratamento de Dados Pessoais.

- A Política de Segurança e Privacidade da Informação é suportada por outras políticas e restante documentação do Sistema de Gestão, incluindo políticas de utilização de recursos, gestão de utilizadores e acessos.
- Todas as políticas que dão suporte à Política de Segurança e Privacidade da Informação têm um responsável atribuído e as revisões às mesmas tem em consideração a visão dos responsáveis de departamento ou direção da organização da *nome_da_organização*.
- O *Information Security Manager* é responsável pela manutenção da Política de Segurança e Privacidade da Informação e pelo suporte e aconselhamento durante a sua implementação, devendo suportar as suas ações nos requisitos da gestão de topo e outras partes interessadas relevantes (e.g., DPO).
- Todos os responsáveis de departamento e direção são responsáveis pela implementação e cumprimento da Política de Segurança e Privacidade da Informação nas suas respetivas áreas.
- A Política de Segurança e Privacidade da Informação está alinhada com a estratégia de gestão do risco definida no Sistema de Gestão da *nome_da_organização*.
- O critério de avaliação dos riscos utilizado na metodologia do cálculo de risco definida no SGSPI baseia-se no valor do ativo em termos de impacto para o Negócio, Privacidade, Segurança da Informação e Cibersegurança, bem como, na possibilidade da ocorrência do evento com base em fatores anteriormente observados e na sua causa potencial.
- A gestão de topo está comprometida em determinar e satisfazer os requisitos de todas as partes interessadas e em melhorar de forma contínua o SGSPI.

- Os objetivos de segurança e privacidade da informação são estabelecidos pelo *Information Security Manager* e pelo *Data Protection Oficer*, tendo em consideração os requisitos e os riscos de segurança e privacidade da informação, sendo aprovados e revistos pela Comissão de Segurança e Privacidade da Informação.
- As comunicações internas e externas relevantes para o SGSPI (e.g., introdução de uma nova política, novo controlo de proteção de dados que afete de modo relevante processos da organização) são efetuadas pela direção de comunicação, através dos canais oficiais, no tempo e frequência ditados pela gestão de topo ou por outros cargos relevantes (e.g., DPO, ISM).
- A gestão da *nome_da_organização* inicia de forma regular a revisão independente do SGSPI por forma a assegurar continuadamente, a efetiva e adequada aptidão da Segurança e Privacidade da Informação..
- A Política de Segurança e Privacidade da Informação é revista anualmente, ou sempre que ocorram alterações que o justifiquem, pela Comissão de Segurança e Privacidade da Informação , nomeadamente, alterações de negócio que incluam fusões, aquisições ou novas parcerias, bem como, nova legislação ou regulamentos e evoluções tecnológicas.
- O cumprimento da Política de Segurança e Privacidade da Informação é obrigatório e o seu não cumprimento poderá resultar em ação disciplinar.
- Em caso de conflito entre qualquer documentação do SGSPI, os colaboradores e as outras partes interessadas, deverão aplicar o documento que melhor garanta a confidencialidade, integridade e disponibilidade da informação, assim como, a proteção dos direitos e liberdades dos titulares.
- Documentação que dá suporte à Política de Segurança e Privacidade da Informação:
  - Política de Tratamento de Dados Pessoais;
  - Política de Classificação e Tratamento da Informação;
  - Política de Segurança e Privacidade Para Terceiras Partes;
  - Política de Utilização de Recursos;
  - Política de Controlo de Acessos;
  - Política de Recursos Humanos;

    - Política de Segurança de Redes;
    - Política de Segurança de Sistemas;
    - Política de Segurança Física e Ambiental;
    - Organização de Segurança e Privacidade da Informação.

- *Assinar uma declaração, por parte dos colaboradores, em que concordam ter lido e vão seguir, as políticas e procedimentos relevantes*: o consentimento pode ser obtido via múltiplas formas e canais, como o correio eletrónico, formulário em linha ou qualquer outro suporte escrito. Exemplo de texto a ser apresentado aos colaboradores:

  Declaro que li, compreendi e tomei consciência[2] de todas as Políticas definidas no Sistema de Gestão da *nome_da_Organização* relativas aos diferentes referenciais normativos e regulamentos, nomeadamente:

  – Política de Segurança e Privacidade da Informação.

  Descrever outras políticas, procedimentos, códigos internos, códigos de ética, etc.

2 Nota do autor: não se solicita a anuência ao colaborador, devido ao desproporcional de forças com a entidade patronal, e como tal, não poder ser dada de forma livre e inequívoca, mas somente a tomada de conhecimento.

X

APÊNDICE X — DESENVOLVER UM PLANO PARA DESASTRES E INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Ter um plano de tratamento de incidentes de segurança é crucial, por permitir a uma organização responder rápida e efetivamente às violações de segurança e minimizar danos reputacionais e financeiros.

Entregáveis[1]:

Desenvolver um Plano para Desastres e Incidentes de Segurança da Informação

- *Definir papéis e responsabilidades*: depende da dimensão, natureza e objeto social da sociedade. O exercício da próxima tabela ilustra papéis e responsabilidades a considerar.

1 Nota do autor: as ações autoexplicativo estão suprimidas.

Tabela 82: Papéis e Responsabilidades

Papel	Responsabilidade	TdM
Especialista em Comunicação Corporativa	Elaboração e gestão dos comunicados internos e externos às partes interessadas. Proteger a reputação da empresa é o objetivo primordial.	NP
Especialista em Recursos Humanos	Tópicos relacionados com possíveis impactos na esfera dos colaboradores.	NP
Especialista Jurídico	Aconselhamento sobre assuntos legais e regulamentares, dependendo da extensão e tipo de dano infligido à organização.	NP
Especialista da CNPD	Aconselhamento técnico e processual.	NP
Especialista do CNCS	Apoio técnico e processual.	NP
Especialista da PJ	Suporte técnico e processual.	NP
Gestor de continuidade	Envolvimento na ocorrência de incidentes, que coloquem em causa a continuidade da infraestrutura de suporte ao negócio da organização.	NP
Gestor de capacidade	Envolvimento na ocorrência de incidentes, que coloquem em causa a capacidade de resposta da infraestrutura de suporte ao negócio da sociedade.	NP
Gestor de disponibilidade	Envolvimento na ocorrência de incidentes, que coloquem em causa a alta disponibilidade da infraestrutura de suporte ao negócio da organização.	NP
Patrocinador (*sponsor*) da Gestão de Topo	Suporte a decisões críticas, como evocar o plano de continuidade de negócios ou desligar parte substancial do ecossistema.	NP
CISO	Suporte sobre decisões críticas.*Interface* com o CNCS e PJ.	NP
DPO	Assuntos relacionados com a proteção dos dados pessoais dos titulares envolvidos. Interface com a CNPD.	NP
Dono do Ativo	Decisões sobre o ativo, como desligá-lo, ou prestar informações sobre os dados processados.	NP
Gestor do Ativo	Decisões operacionais do ativo, como interações com outros ativos ou fornecimento de credenciais.	NP
Embaixador de cibersegurança em cada filial e unidade de negócio\departamento de maior dimensão	Interface de contacto entre a equipa CSIRT e a filial ou unidade de negócio. Muitas vezes, traduz requisitos técnicos em linguagem de negócio, não técnica.	NP
Responsável do CSIRT	Gestor da equipa de resposta a incidentes.	P
Analista Forense	Análise forense, tratamento de evidências digitais, recuperação de informação, investigação da pegada digital e salvaguarda da integridade da prova recolhida para admissibilidade em tribunal.	P
Analista *Threat Hunting*	Monitorização, pesquisa, classificação e análise de eventos de segurança. Foco na pesquisa de indicadores de compromisso e na prevenção de ameaças no ecossistema da organização.	P
Analista de Segurança *Tier* 1	Monitorização, pesquisa, classificação e análise de eventos de segurança. Foco na triagem.	P
Analista de Segurança *Tier* 2	Análise detalhada aos eventos suspeitos, para determinar a natureza da ameaça e extensão de comprometimento nos sistemas da sociedade. Ações de contenção e remediação durante ou após a ocorrência de um incidente.	P
Analista de vulnerabilidades e intrusão (*pentesting*)	Testar as defesas da organização. Posteriormente às intrusões, perpetuadas por atores maliciosos, mapear os passos executados.	P
Assistentes de Resposta a Incidentes	Assistir os Gestores de Reposta a Incidentes. Durante a ocorrência de um incidente, documentam todos os detalhes para posterior análise pós-incidente e melhoria contínua. Também podem realizar ações de reposta a incidentes de complexidade não elevada.	P
Gestores de Resposta a Incidentes	Responsáveis pelas ações de resposta a cada incidente (e.g., *playbooks*), pela sua documentação e envolvimento de todas as partes necessárias.	P

Legenda: TdM - Tipo de Membro [NP - Não Permanente, P - Permanente]

- *Determinar o que fazer com os dados e o sistemas de informação, em caso de incidente.*: o processo de resposta é baseado em documentação da NIST e CISA, encontrando-se explanado na figura ulterior.

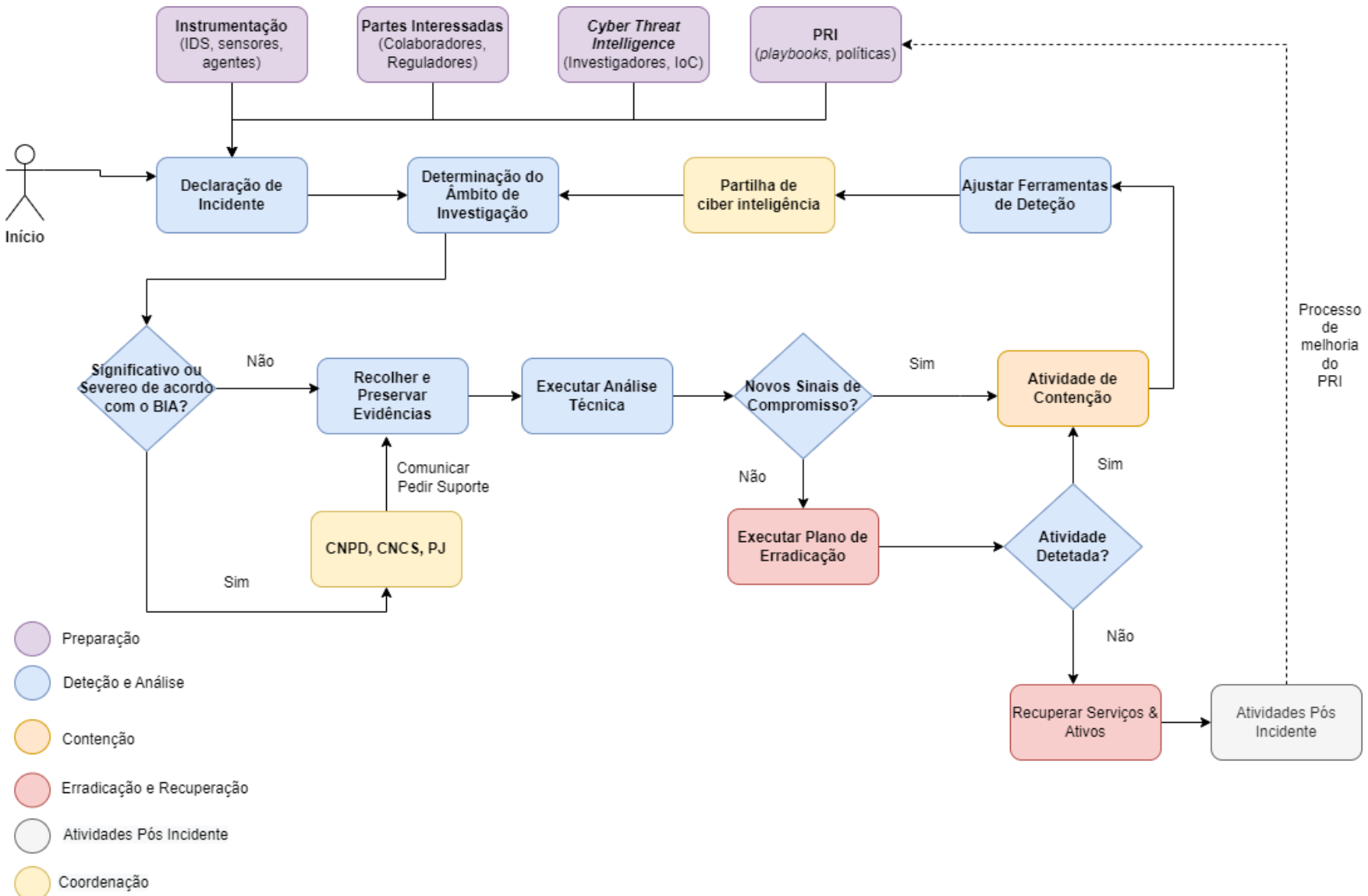


Figura 57: Processo de Resposta a Incidentes

- **Fase de preparação**: consiste na execução conjunto de atividades antes da ocorrência de um incidente:
  - Preparar a documentação necessária à resposta de um incidente (e.g., *playbooks*);
  - Instrumentação (e.g., diagramas de rede, EDR, DLP, IDPS, SIEM);
  - Assegurar que a equipa CSIRT tem o treino e capacidade de resposta a incidentes;
  - Monitorização de *feeds* de inteligência sobre indicadores de ameaças, vulnerabilidades etc.
- **Fase de deteção e análise**: temos as seguintes atividades:
  - Declaração de incidente — comunicar a ocorrência do incidente usando um dos múltiplos canais disponíveis;
  - Determinação do âmbito de investigação — usar os dados disponíveis (e.g., *logs*, artefactos de rede — *firewall*, *proxy*, dados de ligações de rede, registos de atividades dos utilizadores) para identificar o tipo de acesso, a extensão de afetação do ativo ou ativos, o nível de privilégio obtido pelo ator malicioso e o impacto operacional;
  - Recolher e preservar evidências — as evidências devem ser recolhias para poderem ser usadas em processo judicial e para permitir a verificação, categorização, priorização, mitigação, atribuição e relatório do incidente;
  - Executar análise técnica — consiste em correlacionar eventos; criar uma linha temporal de todas as descobertas relevantes; identificar atividades anómalas; recolha de indicadores de compromisso; descobrir a causa raiz e as condições que permitiram o acesso malicioso ao ambiente; mapear o ataque às táticas, técnicas e procedimentos da framework ATT&CK[2] para descobrir o "porquê", "o quê" e "como"; validar e refinar o âmbito de investigação. Perguntas-chave que devem ser respondidas:
    - Qual foi o vetor de ataque inicial (i.e., como o ator malicioso ganhou o acesso inicial ao ecossistema)?;
    - Como o ator malicioso acede ao ambiente?;
    - Está o ator malicioso a explorar vulnerabilidades para conseguir o acesso ou privilégio?;

2 https://attack.mitre.org/

- Como o adversário mantém o comando e o controlo?;
- O adversário tem persistência na rede ou dispositivo?;
- Qual é o método de persistência (e.g., *malware backdoor*, *webshell*, credenciais legítimas, ferramentas remotas)?;
- Que contas foram comprometidas e qual o seu nível de privilégio (e.g., *domain admin*, *local admin*, conta de utilizador)?;
- Qual o método usado para reconhecimento? — descobrir o método pode providenciar uma oportunidade para detetar e determinar a intenção.;
- Há suspeitas ou é conhecido o movimento lateral?;
- Como o movimento lateral é executado (e.g., RDP, partilhas de rede, *malware*)?;
- Exfiltração de dados ocorreu e, se sim, de que tipo e via qual mecanismo?.

* Suporte de Reguladores: quando um incidente é significativo ou severo, é de todo o interesse do banco comunicar e ativar o protocolo de suporte dos reguladores;
* Ajustar ferramentas: aumentar a eficácia das táticas defensivas e preventivas (e.g., atualizar assinaturas IOC), significa tornar os ataques mais complexos e difíceis de executar por parte dos atores maliciosos.

– **Fase de Contenção**: é uma atividade prioritária para a resposta a incidentes, especialmente para os de maior impacto. O objetivo é bloquear dano adicional e remover os acessos dos atores maliciosos. A estratégia ou resposta a adotar depende do cenário (tipo de incidente) e do BIA[3] do ativo. A contenção tem de englobar toda a atividade adversária. Se novos sinais de comprometimento forem encontrados, é necessário balizar novamente o âmbito, caso contrário, podemos passar à próxima fase.
As atividades de contenção incluem:

* Isolamento de sistemas/ativos e segmentos de rede envolvidos no incidente uns dos outros e/ou de recursos não afetados;
* Captura de imagens forenses para preservar evidências e investigação adicional do acidente;

3 Conferir o apêndice V

    - Atualização de regras e filtragem das *firewall*;;
    - Bloqueio de acessos não autorizados;
    - Interrupção de fontes de malware;
    - Fechar portos específicos de servidores/serviços;;
    - Revogação de acessos privilegiados e alteração de segredos de contas privilegiadas (e.g., *system admin*), rotação de chaves privadas e senhas de contas de serviços se estiverem sob suspeita de comprometimento;
    - Direcionar o adversário para uma *sandbox*, de modo a monitorizar as suas atividades, reunir evidência adicional e identificar vetores de ataques.

- **Fase de Erradicação e Recuperação**: a finalidade é o retorno às operações normais pela eliminação dos artefactos maliciosos e mitigação das vulnerabilidades ou outras condições exploradas.
  Atividades de erradicação:
    - Remediação de todas as componentes na nuvem infetadas;;
    - Reconstrução dos sistemas via IAC;
    - Substituição de ficheiros comprometidos com versões limpas;;
    - Instalação de *patching*;
    - Troca de senhas em contas comprometidas;
    - Monitorização de quaisquer sinais de resposta adversa às atividades de contenção;
    - Desenvolvimento de cenários de resposta a vetores de ataques alternativos;
    - Permitir tempo suficiente para assegurar que todas as componentes estão limpas, de todos os mecanismos persistentes (e.g., *backdoors*), visto os atores maliciosos poderem usar mais do que mecanismo.
- Atividades de recuperação:
    - Reconexão ou construção de componentes na nuvem;
    - Estreitar a segurança de perímetro (e.g., regras de *firewall*, regras de acesso *zero trust*);
    - Testar componentes da nuvem, incluindo controlos de segurança;

    - Monitorizar as operações para comportamentos não normais.

  - **Atividades pós incidente**: consiste nas seguintes tarefas:

    - Ajustar sensores, alertas e recolha de registos para evitar repetições de cenários que usaram com sucesso certas táticas, técnicas e procedimentos;
    - Emular táticas, técnicas e procedimentos usados pelos atores maliciosos para verificar a eficácia das contra medidas adotadas;
    - Responder formalmente aos reguladores no caso de incidentes significativos ou severos;
    - Registar a causa raiz e o processo de eliminação da mesma;
    - Identificar processos a melhor no PRI;
    - Verificar a existência de melhorias na capacidade de resposta da equipa.

- *Delinear quem chamar em caso de um incidente*: os incidentes em que não haja alto dano para o negócio e/ou os direitos e liberdades dos indivíduos necessitam somente dos membros "permanente". Nas situações críticas, os membros "não permanente" precisam de ser evocados. Observar o apêndice V.
- *Decidir os tipos de atividades, que constituem um incidente de segurança da informação.*: recomendado a adoção da taxonomia[4] desenvolvida pela Rede Nacional CSIRT[5].

Instalar Supressores de Pico de Tensão e Fontes de Alimentação Ininterrupta

- *Assegurar que cada computador e dispositivos críticos de rede estão conectados a uma UPS*: na aquisição de uma UPS há um conjunto de características a observar:

  - *backup* de baterias;
  - Supressor de picos de tensão;
  - Regulação automática de voltagem;
  - Capacidade de *watts* ou *volt-ampers* suficente;
  - Capacidade temporal em fornecer energia ao equipamentos conectados;
  - Consola de monitorização e gestão;

4 https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.0.pdf
5 https://www.redecsirt.pt/

- Alarmística sonora e de envio de mensagens (e.g., correio eletrónico);
- Opções de conectividade (e.g., *ethernet*, USB).

APÊNDICE Y — PROTEGER OS PONTOS DE ACESSO SEM FIOS E AS REDES

A utilização de algoritmos criptográficos modernos, é a solução mais eficaz na proteção dos dados e informação de terceiros mal-intencionados, independentemente do protocolo de transmissão usado e se o fluxo de conhecimento está em trânsito ou em repouso.

Entregáveis[1]:

Proteger os Pontos de Acesso sem Fios e as Redes

- *Assegurar que o acesso internet sem fios providenciado aos clientes, é separado do da rede corporativa*: os clientes, parceiros e fornecedores, quando se encontram nas instalações corporativas, somente devem ter acesso à *internet* pelo meio de um *captive portal*, garantindo-se assim isolamento da rede corporativa, aceitação da política de segurança e privacidade, e traçabilidade das atividades de navegação em caso de fraude e ilícitos.
  Um possível *disclaimer*:

  AVISO LEGAL — Navegação na Internet

  Nota de Segurança

  A utilização do recurso de *internet* da *nome_da_empresa* e suas participadas, doravante *nome_abreviado_da_empresa*, deverá nortear-se por uma utilização responsável e de âmbito profissional, não sendo consideradas utilização responsável / profissional, situações que interfiram ou possam interferir, lesivamente, com outros utilizadores ou serviços, sejam eles internos ou externos à *nome_abreviado_da_empresa*, nomeadamente:

  a) com o propósito do exercício de atividades ilegais ou ilegítimas;
  b) com o propósito de desrespeitar a integridade física e moral dos utilizadores em particular, em atos de promoção de assédio, xenofobia, terrorismo ou difamação;
  c) para criação, transmissão ou acesso a conteúdos sem respeito pelos direitos de propriedade intelectual, *copyright* ou *trademark*;

1 Nota do autor: as ações autoexplicativo estão suprimidas.

d) para o exercício de atividades privadas, incluindo mineração de criptomoedas e venda de serviços e produtos;
e) para obter ou tentar obter acesso não autorizado, para identificar vulnerabilidades, em sistemas ou infraestruturas tecnológicas;
f) outras situações que não estando discriminadas anteriormente possam interferir com a segurança das infraestruturas e a sua utilização responsável.

Nota de Privacidade

Responsável pelo Tratamento — *nome_abreviado_da_empresa.*
Finalidades — manter a segurança dos nossos serviços; gestão dos meios tecnológicos da empresa.
Fundamento legal — Interesses legítimos prosseguidos pelo responsável pelo tratamento. Considerando 49 do Regulamento (UE) 2016/679.
Categoria de dados pessoais tratados — Endereço IP do destinatário, Endereço IP do remetente; Data e hora de início e fim da conexão; Análise do tráfego (em caso de evento de segurança).
Forma de exercício do direito de acesso — Por solicitação escrita (*indicar canal de correio eletrónico, website, ou outro*) ou pessoal.
Interconexões ou decisões automatizadas — não há.
Comunicação de dados — não há.
Fluxo transfronteiriço de dados — não há.
Prazo máximo de conservação dos dados — 6 meses.
Segurança dos dados — São aplicadas medidas técnicas e organizativas adequadas para assegurar um nível de segurança apropriado ao risco por manter em arquivo eletrónico os Dados Pessoais dos visitantes.
Reclamação — O visitante tem o direito de apresentar reclamação a uma Autoridade de Controlo da União Europeia relativamente à proteção dos seus Dados Pessoais.

- *Implementar uma VPN em caso de necessidade de ligação a uma rede desconhecida ou trabalhar a partir de casa.*: idealmente, em vez de uma VPN, a implementação de uma solução SSE oferece um nível de proteção superior por albergar diferentes componentes, nomeadamente, SWG, CASB e ZTNA. A solução da *Zscaler*[2] é uma excelente opção.

Eliminação Segura de Computadores Obsoletos e Suportes de Armazenamento

- *Instalar uma aplicação de limpeza remota nos computadores, tablets, telemóveis, e outros dispositivos móveis.* : conferir o apêndice R.

2 https://www.zscaler.com/products/zscaler-private-access

- *Na erradicação de papéis com informação sensível, usar um triturador de papel.*: optar por um triturador de nível P4, ou seja, que ofereça uma superfície máxima de corte transversal das partículas de 160 mm² com uma largura máxima de tira de 6 mm, conforme as especificações do DIN 66399[3].

3 https://www.din.de/en/getting-involved/standards-committees/nia/publications/wdc-beuth:din21:155420083

Z

APÊNDICE Z — USAR CRIPTOGRAFIA PARA INFORMAÇÕES CONFIDENCIAIS DE NEGÓCIO

Todos os fluxos de informação, independentemente de se encontrarem em trânsito (e.g., acesso a um *website*) ou em repouso (e.g., base de dados), são fundamentais estarem protegidos recorrendo a tecnologia de encriptação. Somente protocolos modernos criptográficos devem ser utilizados. A utilização incorreta de algoritmos de encriptação pode resultar em exfiltração de dados sensíveis, divulgação de chaves, quebra de autenticação, sessão insegura, e ataques de adulteração de identidade. A figura sequente ilustra os requisitos mínimos a serem observados: (OWASP, 2020)

```
Key exchange: Diffie-Hellman key exchange with minimum 2048 bits
Message Integrity: HMAC-SHA2
Message Hash: SHA2 256 bits
Asymmetric encryption: RSA 2048 bits
Symmetric-key algorithm: AES 128 bits
Password Hashing: PBKDF2, Scrypt, Bcrypt
ECDH, ECDSA: 256 bits
```

Figura 58: Requisitos mínimos criptográficos

Entregáveis[1]:

- *Cifrar a totalidade dos discos — que encripta toda a informação nos meios de armazenamento — em todos os computadores, tablets, e telefones inteligentes.*: para os sistemas *Windows* utilizar a tecnologia *Bitlocker*[2]. No que respeita ao *Linux*, optar pela tecnologia *VeraCrypt*[3].
- *Guardar uma cópia da palavra-passe de encriptação ou chave, numa localização segura e separado do local onde as cópias de segurança são armazenadas*: utilizar um gestor de palavras-passe como descrito no apêndice P.
- *Encriptar o enviar documentos ou e-mails sensíveis.*: dois excelentes serviços de correio eletrónico, que providenciam encriptação ponto a ponto, são o *Pro-*

1 Nota do autor: as ações autoexplicativo estão suprimidas.
2 https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-basic-deployment
3 https://www.veracrypt.fr/en/Home.html

tonMail[4] e *Tutanota*[5]. Alternativas seguras a modelos baseados em anúncios, como no caso do *Gmail* e *Outlook*, que ativamente varrem as caixas de correio, como o intuito de entregarem anúncios relevantes.
No caso de instalação local, para *Windows* aconselha-se o GPG4WIN[6], enquanto para *Linux* o GNUPG[7] é uma escolha acertada.

4 https://proton.me/mail
5 https://tutanota.com/
6 https://www.gpg4win.org/index.html
7 https://gnupg.org/

DECLARAÇÃO

Declaro, sob compromisso de honra, que o trabalho apresentado nesta dissertação, com o título *"Manual Prático para PME - Cibersegurança, Segurança da Informação, Privacidade e Proteção de Dados Pessoais"*, é original e foi realizado por Miguel Ângelo Saragoça Soares (2210259) sob orientação de Professor Doutor Mário Antunes (mario.antunes@ipleiria.pt), Professora Doutora Marisa Maximiano (marisa.maximiano@ipleiria.pt) e Professor Ricardo Gomes (ricardo.p.gomes@ipleiria.pt).

Assinado por: **Miguel Ângelo Saragoça Soares**
Num. de Identificação: 10303237
Data: 2023.09.19 21:53:30+01'00'

Leiria, Setembro de 2023

Miguel Ângelo Saragoça Soares