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

IMPLEMENTAÇÃO DE UM SISTEMA DE GESTÃO DE SEGURANÇA DE INFORMAÇÃO (SGSI) BASEADO NA NORMA ISO/IEC 27001 NA EIB,SA

ESTUDANTE SÉRGIO LOPES LAVOS

Leiria, Setembro de 2023

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

IMPLEMENTAÇÃO DE UM SISTEMA DE GESTÃO DE SEGURANÇA DE INFORMAÇÃO (SGSI) BASEADO NA NORMA ISO/IEC 27001 NA EIB,SA

ESTUDANTE SÉRGIO LOPES LAVOS
Número: 2200343

Projeto realizado sob orientação do Professor Doutor Leonel Filipe Simões Santos
(leonel.santos@ipleiria.pt).

Leiria, Setembro de 2023

AGRADECIMENTOS

Gostaria de expressar os meus sinceros agradecimentos às pessoas que me apoiaram ao longo da minha jornada de mestrado.

Agradeço à minha esposa e aos meus filhos por estarem sempre ao meu lado e me terem incentivado e motivado, mesmo nos momentos mais difíceis, sem a sua presença constante e o seu encorajamento, teria sido impossível chegar até aqui.

Com todo o coração, quero expressar a minha sincera gratidão à minha família e amigos próximos pelo seu amor e apoio inabalável.

Agradecer ao meu orientador, Professor Doutor Leonel Simões pela sua orientação, apoio e conselhos valiosos durante todo o processo. Foi um privilégio trabalhar sob a sua supervisão, estou grato por todo o tempo, paciência e dedicação que empenhou na minha tese.

Agradeço também ao Professor Doutor Carlos Rabadão, pela sua valiosa contribuição e orientação, obrigado por partilhar o seu vasto conhecimento e experiência comigo, por me apoiar em todos os momentos e por ser um grande mentor.

Também quero expressar a minha gratidão ao meu patrão, Tiago Coutinho, que me concedeu a flexibilidade necessária para conciliar as minhas responsabilidades profissionais com os estudos de mestrado. A sua confiança e apoio foram cruciais para o sucesso deste projeto.

Por último, mas não menos importante, gostaria de agradecer aos meus colegas de trabalho e de curso, que me ajudaram e incentivaram ao longo deste caminho.

Obrigado a todos por fazerem parte desta jornada e por tornarem esta experiência memorável e gratificante.

Muito obrigado a todos!

RESUMO

A Empresa Industrial de Borracha, S.A. (EIB) é líder nacional na indústria de fabricação de produtos de borracha para pneus e recauchutagem. No entanto, enfrenta desafios significativos no cenário global altamente competitivo e tecnologicamente avançado. A digitalização dos processos e a interconexão dos sistemas industriais requerem uma abordagem robusta para garantir a segurança dos sistemas de informação e proteção dos ativos de informação sensíveis da empresa. A integridade dos dados, a confidencialidade das informações e a disponibilidade dos sistemas são cruciais para a continuidade dos negócios e preservação da sua reputação.

Este projeto apresenta o início da implementação de um Sistema de Gestão de Segurança da Informação (SGSI) na Empresa EIB, alinhado com os princípios da norma ISO/IEC 27001. Com foco central na cibersegurança e proteção de dados, o estudo percorreu várias etapas. Inicialmente, houve a caracterização da EIB e uma análise aprofundada das normas e regulamentos vigentes. A implementação do SGSI seguiu de perto os princípios da ISO/IEC 27001, com especial atenção à gestão de riscos e ativos.

A gestão de riscos e ativos, foi alinhada com as diretrizes da ISO/IEC 27005, enriquecida pelo "Guia para Gestão dos Riscos em Matérias de Segurança da Informação e Cibersegurança"do Centro Nacional de Cibersegurança (CNSC). Esta abordagem não apenas acrescenta profundidade à gestão de riscos, mas também reforça a resiliência do SGSI perante as ameaças em constante evolução.

Uma das características deste projeto é a abordagem à avaliação, monitorização e melhoria contínua, fundamentais para a robustez do SGSI. Além do desenvolvimento técnico, destacou-se a promoção do crescimento pessoal, enfatizando a sensibilização e comportamentos seguros em todos os níveis da organização. A governança dos sistemas de TI na EIB foi fortalecida, realçando a interligação harmoniosa entre o SGSI e os sistemas de gestão já estabelecidos ISO 9001 e ISO 14001.

A implementação do SGSI na EIB tem produzido resultados consideráveis, no estabelecimento de políticas e procedimentos sólidos, na integração coesa com sistemas de

gestão existentes, na crescente consciencialização organizacional relativamente à segurança da informação, na definição de abordagens para a gestão de riscos e na garantia de conformidade com normas e regulamentos.

Uma vez que o mercado de SGSI é dominado por empresas de consultoria, a implementação por quadros internos das organizações representa um desafio significativo. Embora existam muitos regulamentos e diretrizes disponíveis, adaptá-los à realidade específica de cada organização sem guiões ou modelos já pré-definidos pode revelar-se uma tarefa bastante complexa.

Embora o foco não seja a procura imediata pela certificação ISO/IEC 27001, este projeto reforça a importância de práticas de segurança normalizadas e sustentáveis. Ao promover a consciencialização e a adoção de comportamentos seguros, o SGSI está bem posicionado para enfrentar os desafios sempre em evolução do ambiente empresarial e digital, contribuindo para a proteção dos ativos e informações valiosas da organização.

Palavras-chave: Sistema de gestão de segurança da informação (SGSI), ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005

ABSTRACT

The Empresa Industrial de Borracha, S.A. (EIB) is a Portuguese leader in the manufacturing of rubber products for tires and retreading. However, it faces significant challenges in the highly competitive and technologically advanced global landscape. The digitization of processes and interconnection of industrial systems require a robust approach to ensure the security of information systems and protection of the company's sensitive information assets. Data integrity, information confidentiality, and system availability are crucial for business continuity and preservation of its reputation.

This project presents the initiation of the implementation of an Information Security Management System (ISMS) at EIB Company, aligned with the principles of ISO/IEC 27001. With a central focus on cybersecurity and data protection, the study progressed through various stages. Initially, the characterization of EIB and an in-depth analysis of current norms and regulations were conducted. The ISMS implementation closely adhered to the principles of ISO/IEC 27001, with special attention given to risk and asset management.

The risk and asset management were aligned with ISO/IEC 27005 guidelines, enriched by the "Guide for Risk Management in Information Security and Cybersecurity"from the Portuguese National Cybersecurity Center (CNSC). This approach not only enhances the depth of risk management but also reinforces the resilience of the ISMS against evolving threats.

One of the distinguishing features of this project is its approach to assessment, monitoring, and continuous improvement, which are critical for the robustness of the ISMS. Beyond technical development, the promotion of personal growth was emphasized, highlighting awareness and secure behaviors at all organizational levels. The governance of IT systems at EIB was strengthened, emphasizing the seamless integration between the ISMS and the established ISO 9001 and ISO 14001 management systems.

The implementation of the ISMS at EIB has yielded significant results in the establishment of robust policies and procedures, seamless integration with existing management

systems, the growing organizational awareness regarding information security, the definition of approaches for risk management, and ensuring compliance with standards and regulations.

Since the ISMS market is dominated by consulting firms, implementing it with internal staff within organizations poses a significant challenge. Although there are many regulations and guidelines available, adapting them to the specific reality of each organization without predefined scripts or templates can prove to be a rather complex task.

While immediate ISO/IEC 27001 certification may not be the primary focus, this project underscores the significance of standardized and sustainable security practices. By fostering awareness and the adoption of secure behaviors, EIB's ISMS is well-positioned to address the ever-evolving challenges of the business and digital environment, contributing to the safeguarding of the organization's valuable assets and information.

Keywords: Information Security Management System (ISMS), ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005

ÍNDICE

Agradecimentos i
Resumo iii
Abstract v
Índice vii
Lista de Figuras xiii
Lista de Tabelas xv
Lista de Abreviaturas xvii

1 Introdução 1
1.1 Caso de Estudo . . . 1
1.2 Âmbito do Projeto . . . 2
1.3 Objectivos . . . 3
1.4 Motivação, Contribuição e Inovação . . . 4
1.5 Metodologias . . . 5
1.6 Resultados Esperados . . . 6
1.7 Estrutura do documento . . . 7
2 Revisão bibliográfica 9
2.1 Sistema de Gestão da Segurança da Informação (SGSI) . . . 9
2.1.1 Impacto da certificação ISO/IEC 27001 . . . 12
2.1.2 Vantagem competitiva . . . 13
2.1.3 Áreas de segurança da informação . . . 14
2.1.4 Políticas e procedimentos de segurança da informação . . . 15
2.1.5 Gestão de riscos . . . 15
2.2 Leis e Regulamentos . . . 17
2.2.1 Lei do Cibercrime - Lei n.º 109/2009 . . . 17
2.2.2 Segurança das Redes e de toda a informação - Lei n.º 46/2018 . . . 17
2.2.3 Decreto-Lei n.º 55/2019 . . . 18
2.2.4 Regulamento Geral sobre a Proteção de Dados - RGPD . . . 19

2.3 Normas . . . 21
2.3.1 NP EN ISO 9001 . . . 21
2.3.2 NP EN ISO 14001 . . . 25
2.3.3 NP ISO 31000 . . . 26
2.3.4 ISO/IEC 27001 . . . 28
2.3.5 ISO/IEC 27002 . . . 38
2.3.6 ISO/IEC 27003 . . . 40
2.3.7 ISO/IEC 27005 . . . 42
2.3.8 Outras Normas da família 27000 . . . 44
2.4 Outros Standards e Metodologias . . . 48
2.4.1 IEC 62443 . . . 48
2.4.2 COBIT . . . 50
2.4.3 ITIL . . . 53
2.4.4 NIST . . . 56
2.4.5 Comparação de metodologias . . . 60
2.5 Frameworks Nacionais . . . 61
2.5.1 Quadro Nacional de Cibersegurança . . . 62
2.5.2 Roteiro para Capacidades Mínimas de Cibersegurança . . . 63
2.5.3 Certificação de maturidade digital «Selos digitais» . . . 63
2.6 Trabalho Relacionado . . . 64
2.7 Síntese . . . 68

3 Caraterização do Caso de Uso 71
3.1 Organograma . . . 72
3.2 Sistema de Gestão Integrada . . . 72
3.3 Relação entre Departamentos e Tecnologias de Informação . . . 73
3.4 Componentes Tecnológicos de TI . . . 75
3.4.1 Componentes desatualizados ou obsoletos . . . 78
3.4.2 Camada de apresentação - Intranet . . . 79
3.5 Síntese . . . 81

4 Implementação 83
4.1 Suporte da gestão de topo . . . 83

4.2 Reuniões de Kickoff . . . 85
4.3 Âmbito do SGSI . . . 85
4.4 Justificação de seleção da norma ISO/IEC 27001 . . . 86
4.5 Integração com outros padrões . . . 86
4.5.1 Partes interessadas . . . 87
4.5.2 Ações de formação e consciencialização em SI . . . 88
4.5.3 Comunicação . . . 88
4.5.4 Riscos e oportunidades . . . 90
4.5.5 Análise SWOT . . . 91
4.6 Gestão Documental . . . 93
4.6.1 Objetivos . . . 93
4.6.2 Fluxograma . . . 94
4.6.3 Políticas e procedimentos de SI . . . 94
4.6.4 Outras secções . . . 96
4.6.5 Responsabilidades documentais . . . 97
4.7 Manual de Funções . . . 98
4.8 Análise GAP . . . 102
4.9 Políticas de segurança e procedimentos . . . 104
4.9.1 Políticas de Segurança da Informação . . . 104
4.9.2 Políticas de uso aceitável para recursos de TI . . . 106
4.9.3 Procedimentos de TI . . . 107
4.9.4 Síntese de Políticas e Procedimentos . . . 109
4.10 Declaração de Aplicabilidade (SoA) . . . 109
4.11 Síntese . . . 111

5 Gestão de Riscos 113
5.1 Metodologia Gestão do Risco . . . 113
5.2 Estabelecer o contexto . . . 115
5.3 Gestão de ativos . . . 117
5.3.1 Ativos . . . 117
5.3.2 Classificação e valorização de ativos . . . 118
5.3.3 Ameaças e vulnerabilidades . . . 119
5.3.4 Inventários de ativos . . . 120

5.4 Avaliação de risco . . . 121
5.4.1 Metodologia de avaliação de riscos . . . 122
5.4.2 Metodologia de análise dos riscos . . . 126
5.4.3 Matriz de risco . . . 127
5.4.4 Riscos a tratar . . . 128
5.4.5 Aceitar o risco . . . 129
5.4.6 Transferência de riscos . . . 130
5.5 Controlos de segurança . . . 131
5.6 Matriz de riscos e Oportunidades . . . 132
5.7 Relatório de análise de risco do SGSI . . . 134
5.8 Plano de tratamento de riscos . . . 135
5.9 Comunicação e consulta dos riscos . . . 138
5.10 Monitorização e revisão dos riscos . . . 139
5.11 Gestão de incidentes de SI . . . 140
5.12 Caso uso real - Segregação da rede Zeppelin . . . 142
5.12.1 Estabelecer o Contexto . . . 142
5.12.2 Plano de Tratamento . . . 143
5.12.3 Avaliação e Monitorização . . . 144
5.13 Síntese . . . 145
6 Monitorização, Avaliação, Comunicação e Melhoria contínua 147
6.1 Monitorização do SGSI . . . 147
6.2 Métricas e indicadores de SI . . . 148
6.3 Comunicação . . . 149
6.4 Revisão do SGSI . . . 150
6.5 Auditorias Internas . . . 152
6.6 Formação e Consciencialização . . . 153
6.7 Simulacros e Plano de Simulacros . . . 154
6.8 Melhoria continua . . . 156
6.8.1 Fator Humano . . . 157
6.8.2 Novas Ferramentas/Tecnologias . . . 158
6.8.3 Leis e Regulamentos . . . 159
6.9 Conformidade com metodologias adotadas . . . 160
6.9.1 Documentos e registos obrigatórios da ISO/IEC 27001 . . . 160

6.9.2 Roadmap Integrity 165
6.10 Síntese 167

7 Conclusões 169
7.1 Resultados Alcançados 169
7.2 Analise critica 171
7.3 Considerações 171
7.4 Trabalho Futuro 172

Bibliografia 174

Apêndices

A Políticas de Segurança da informação 181
A.1 Política Geral de Segurança da Informação 181
A.2 Política de Backups e Recuperação 187
A.3 Política de Redes 191
A.4 Política de Monitorização e Registo de Eventos 195
A.5 Política de Gestão de Ativos 199
A.6 Política de Acesso e Controlo de Informação 203
A.7 Política de Sensibilização e Formação em SI 207
A.8 Política de Desenvolvimento de Software 210
A.9 Política de Classificação da Informação 213
A.10 Política de Gestão e Eliminação de Suportes de Informação 216
A.11 Política de Controlo Criptográfico 219
A.12 Política de Controlo de Acessos Fisicos 222
A.13 Política de Transferência de informação 225
A.14 Política de Relação com Fornecedores 228
A.15 Política de Gestão de Riscos 231
B Políticas de uso aceitável 235
B.1 Leis e Normas 235
B.2 Papeis e Responsabilidades 237
B.3 Manutenção de Postos e Ambiente de Trabalho 241
B.4 Correio Eletrónico Empresarial 246

B.5 Navegação na internet 249
B.7 Ética e Privacidade 254
B.8 Software e Licenças 257
B.9 Trabalho Remoto 260
B.10 BYOD (Bring Your Own Device) 264
B.11 Gestão de Passwords 267
B.12 Segurança de Dados Pessoais 270
B.13 Incidentes de Segurança da Informação 274
C Procedimentos de TI 277
C.1 Operações com Utilizadores 277
C.2 Registo de Incidentes de segurança da informação 280
D Declaração de Aplicabilidade 285
E Auditoria de Diagnóstico 301

Declaração 307

LISTA DE FIGURAS

Figura 1 Roadmap de Implementação SGSI adaptado de Integrity, 2023 . . 6
Figura 2 Processo Implementação SGSI Ferreira, 2020 11
Figura 3 Representação esquemática, elementos de um processo simples (*NP ISO 9001* 2015) 23
Figura 4 Representação da ISO 9001 no ciclo PDCA (*NP ISO 9001* 2015) 24
Figura 5 Relações entre princípios, estrutura e processo da gestão do risco (*NP ISO 31000* 2012) 26
Figura 6 Princípios, estrutura e processo (*ISO 31000* 2018) 27
Figura 7 Processo iterativo PDCA para implementação de um SGSI 29
Figura 8 Requisitos da ISO/IEC 27001 adaptado de (Integrity, 2023) . . . 31
Figura 9 Ciclo PDCA aplicado às cláusulas da ISO/IEC 27001 32
Figura 10 Controlos da ISO/IEC 27001 (Integrity, 2023) 33
Figura 11 Estrutura global da ISO/IEC 27001 fonte adaptada de (Integrity, 2023) 34
Figura 12 Dimensões de segurança da informação da ISO 27001 36
Figura 13 3 pilares da segurança da informação / objetivos de segurança . . 37
Figura 14 Resumo alterações ISO/IEC 27001:2022 baseado em (Kosutic, 2023). 38
Figura 15 Correlação ISO/IEC 27002:2013 e ISO/IEC 27002:2022 (*ISO/IEC 27002* 2022) 40
Figura 16 Processo iterativo de Gestão de Risco ISO 27005 (*ISO/IEC 27005* 2022) 43
Figura 17 Relação entre as famílias da ISO/IEC 27000 adaptado de (*ISO/IEC 27000* 2018) 45
Figura 18 Princípios COBIT (itsmnapratica, 2023) 51
Figura 19 Ciclo de Vida de um Serviço - ITIL (despnet, 2023) 54
Figura 20 Principais funções da NIST (NIST, 2023) 58
Figura 21 Organograma funcional 72
Figura 22 Diagrama dependências departamentais e TI 74

Figura 23 Heterogeneidade de componentes tecnológicos 76
Figura 24 Plano comunicações EIB 89
Figura 25 Fluxograma documental da EIB 94
Figura 26 Responsabilidades de elaboração, aprovação e arquivo de documentos do SIG EIB 98
Figura 27 Processo de Gestão de Risco, adapatado de (*ISO/IEC 27005* 2022)115
Figura 28 Excerto de Matriz de Riscos e Oportunidades da EIB 133
Figura 29 Tratamento dos Riscos ISO/IEC 27005 (Centro Nacional de Cibersegurança, 2023) 137
Figura 30 Ativo com risco superior a nove 142
Figura 31 Documentos e registos da ISO/IEC 27001:2013 (Ghazvini et al., 2018) 161
Figura 32 Formulário de Registo de Incidentes de SI no GLPI 283

LISTA DE TABELAS

Tabela 1 Controlos de Referência / Categorias / Controlos ISO/IEC 27001:2013 (Correia, 2016) . . . 35
Tabela 2 Termos e definições da ISO/IEC 27000 (*ISO/IEC 27000* 2018) . 47
Tabela 3 Comparação entre ITIL, COBIT, NIST e ISO 27001 . . . 61
Tabela 4 Exemplo inventario de ativos valorizado e classificado . . . 121
Tabela 5 Categorias de classificação da probabilidade . . . 123
Tabela 6 Categorias de classificação do Impacto . . . 126
Tabela 7 Matriz de riscos . . . 127
Tabela 8 Níveis de criticidade . . . 128
Tabela 9 Tratamento dos riscos EIB . . . 136
Tabela 10 Tratamento dos riscos (Centro Nacional de Cibersegurança, 2023) 138
Tabela 11 Mapeamento entre documentos obrigatários da norma ISO/IEC 27001 e documentos desenvolvidos no âmbito do SGSI da EIB . . 163
Tabela 12 Mapeamento entre documentos **não obrigatários** da ISO/IEC 27001 e documentos desenvolvidos no âmbito do SGSI da EIB . . 164
Tabela 13 Tempos definidos no roadmap Integrity . . . 165
Tabela 14 Mapeamento entre roadmap Integrity e documentos desenvolvidos no SGSI . . . 167
Tabela 15 Declaração de aplicabilidade . . . 300

LISTA DE ABREVIATURAS

2FA	Two-factor authentication.
ABC	A lista de acrónimos deve ficar ordenada alfabeticamente.
ACL	Access Control List.
AD	Active Directory.
ADSL	Assimetric Digital Subscriber Line.
AS400	IBM Application System/400.
ASCII	American Standard Code for Information Interchange.
BIOS	Basic Input/Output System.
bit	Digito binário.
Byte	Unidade de informação digital composta por oito bits.
CIA	Confidentiality, Integrity, Availability.
CMMS	Computerized Maintenance Management System.
CNCS	Centro Nacional de Cibersegurança.
CODEC	COmpression/DECompression.
CPU	Central Processing Unit.
DA	Declaração de Aplicabilidade.
DHCP	Dynamic Host Configuration Protocol.
DLL	Dynamic Link Library.

DNS	Domain Name System.
DSI	Departamento de Segurança da Informação.
DSSI	Departamento de Segurança de Sistemas de Informação.
DTI	Departamento de Tecnologias da Informação.
EDR	Endpoint Detection and Response.
EMAS	Environmental Management and Audit Scheme.
ERP	Enterprise Resource Planning.
FTP	File Transfer Protocol.
GLPI	Gestionnaire Libre de Parc Informatique.
HRMS	Human Resource Management System.
ICS	Industrial control system.
IDS/IPS	Intrusion Detection and Prevention Systems.
IoT	Internet of Things.
IP	Internet Protocol.
IPAC	Instituto Português de Acreditação.
ISO 14001	Grupo de normas que estabelecem diretrizes sobre a área de gestão ambiental.
ISO 9001	Grupo de normas técnicas que estabelecem um modelo de gestão da qualidade.
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission.
ISO/IEC 27000	Normas da família ISO/IEC 27000 convergem para o Sistema de Gestão de Segurança da Informação.
ISO/IEC 27001	Padrão para sistema de gestão da segurança da informação.
ISO/IEC 27002	Norma de boas práticas para gestão de segurança da informação.
ISO/IEC 27003	Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Orientações.

ISO/IEC 27005	Técnicas de Segurança — Gestão de risco de segurança da informação.
ISP	Internet Service Provider.
ITIL	Information Technology Infrastructure Library.
MAGERIT	Metodologia de Análise e Gestão de Riscos de Sistemas de Informação.
MES	Manufacturing Execution System.
MFA	multi-factor authentication.
NAS	Network-attached storage.
NIST	US National Institute of Standards and Technology.
NIST CF	National Institute of Standards and Technology Cybersecurity Framework.
NTA	Network Traffic Analysis.
PDCA	PLAN - DO - CHECK - ACT, método iterativo de gestão de quatro passos, utilizado para o controlo e melhoria contínua.
QNC	Quadro Nacional de Cibersegurança.
RAS	Remote Access Service.
RGPD	Regulamento Geral de Proteção de Dado.
SCADA	Supervisory Control and Data Acquisition.
SFP	Small Form-factor Pluggable.
SGA	Sistema de gestão ambiental.
SGI	Sistema de Gestão Integrado.
SGQ	Sistema de gestão da qualidade.
SGSI	Sistema de Gestão de Segurança da Informação.
SI	Sistemas de Informação.

SIEM	Security Information and Event Management.
SIGs	Sistemas Integrados de Gestão.
SO	Sistema Operativo.
SoA	Statement of Applicability.
SWOT	Strengths, Weaknesses, Opportunities, Threats.
TCP	Transmission Control Protocol.
TI	Tecnologias de Informação.
TIC	Tecnologias da Informação e Comunicação.
VLAN	Virtual Local Area Network.
VPN	Visrtual Private Network.
VSS	Volume Shadow Copy Service.

1

INTRODUÇÃO

No atual contexto, é amplamente reconhecido que os sistemas de informação desempenham um papel fundamental nas organizações, permitindo-lhes obter vantagens competitivas em relação aos seus concorrentes e sustentar os seus negócios e processos. No entanto, constata-se que nem sempre é dado o devido investimento na segurança dos sistemas de informação, o que pode resultar em vulnerabilidades e riscos para as organizações.

Infelizmente, quase diariamente surgem notícias de sistemas de informação contaminados por *malware*, invasões de sistemas, incidentes de *ransomware* e fugas de informações sensíveis. Esses incidentes de segurança representam um desafio significativo para todas as organizações, uma vez que colocam em risco a confidencialidade, integridade e disponibilidade das informações, bem como a reputação e a continuidade dos negócios.

Nesse sentido, é crucial consciencializar os decisores sobre os riscos envolvidos e a importância de proteger adequadamente os sistemas de informação. A implementação de um sistema de segurança da informação baseado nas normas da família ISO 27000 surge como uma solução efetiva para garantir a proteção dos ativos de informação e mitigar os riscos associados.

Este documento visa apresentar o projeto de implementação do SGSI na EIB, descrevendo os objetivos, os benefícios esperados e a estrutura geral do sistema. Serão abordados os principais requisitos de segurança da informação, bem como as etapas e os recursos necessários para alcançar a conformidade com as melhores práticas e padrões nomeadamente com a ISO 27001.

1.1 CASO DE ESTUDO

A Empresa Industrial de Borracha, S.A. (EIB) é uma empresa fabricante de produtos de borracha para a indústria de pneus e recauchutagem. Com uma longa história de

excelência e compromisso com a qualidade e ambiente, sendo reconhecida como líder no seu setor.

No entanto, no atual cenário global, altamente competitivo e em constante evolução, a EIB enfrenta desafios significativos para manter uma posição de destaque. A crescente dependência de sistemas de informação e a rápida evolução tecnológica exigem que a empresa esteja preparada para lidar com ameaças de segurança e garantir a devida proteção dos seus ativos de informação.

Com a digitalização dos processos, a adoção de tecnologias avançadas e a interconexão dos sistemas industriais, a segurança dos sistemas de informação tornou-se uma preocupação crucial para a EIB. A integridade dos dados, a confidencialidade das informações sensíveis e a disponibilidade dos sistemas são elementos essenciais para a continuidade dos negócios e a proteção da reputação da empresa.

Diante estes cenários, a implementação de um Sistema de Gestão de Segurança da Informação (SGSI) na EIB é uma medida estratégica e necessária. O SGSI proporcionará uma abordagem estruturada e abrangente para identificar, avaliar e mitigar os riscos de segurança da informação enfrentados pela organização. Este fornecerá um conjunto de políticas, processos e controlos que permitirão à EIB proteger os ativos de informação de forma consistente e efetiva.

1.2 ÂMBITO DO PROJETO

O âmbito da implementação do Sistema de Gestão de Segurança da Informação (SGSI) na EIB assume uma abordagem inicial focada na melhoria da segurança da informação, sem a intenção imediata de obter certificação. Este âmbito é delineado para estabelecer bases sólidas, criar consciencialização e integrar controlos de segurança de forma eficaz, preparando o terreno para futuras etapas de certificação, se necessário. Além disso, o SGSI será integrado harmoniosamente com os sistemas de gestão existentes ISO 9001 e ISO 14001, a fim de garantir uma abordagem abrangente e coerente com a gestão organizacional.

1.3 OBJECTIVOS

O principal objetivo deste projeto é implementar um SGSI que inclua a criação de políticas e procedimentos abrangentes de segurança da informação, integrados com os sistemas de gestão existentes, visando aumentar a consciencialização sobre segurança da informação, melhorar a proteção dos dados e promover uma cultura de cibersegurança.

Como resultado da implementação do SGSI, visam-se alcançar os seguintes objetivos secundários, assentes em três pilares: vantagem competitiva, segurança dos sistemas e conformidade legal e regulatória.

1. **Vantagem Competitiva**
    - Reforçar a posição da EIB no mercado, utilizando a segurança da informação como um diferencial competitivo.
    - Implementar práticas de segurança que garantam a confidencialidade, integridade e disponibilidade dos dados e sistemas da organização.
    - Desenvolver políticas e procedimentos que assegurem a proteção adequada da informação sensível e estratégica da EIB, conferindo-lhe uma vantagem sobre os concorrentes.
2. **Segurança dos Sistemas**
    - Proteger os sistemas de informação da EIB contra ameaças internas e externas, garantindo a continuidade dos negócios e a proteção dos ativos da organização.
    - Identificar e mitigar os riscos de segurança, adotando medidas técnicas, organizacionais e humanas adequadas.
    - Implementar controlos de segurança eficazes, incluindo monitorização, deteção de intrusões e resposta a incidentes, para proteger os sistemas contra ataques cibernéticos e outras ameaças.
    - Identificar e mitigar vulnerabilidades nos sistemas de controlo industrial (ICS), garantindo a continuidade das operações e a segurança dos processos produtivos da EIB.
3. **Conformidade Legal e Regulatória**

- Garantir que a EIB esteja conforme as regulamentações e leis aplicáveis, especialmente aquelas relacionadas com a proteção de dados e privacidade.
- Adotar medidas de segurança que cumpram os requisitos legais e regulatórios, como o Regulamento Geral de Proteção de Dados (RGPD) e outras normas setoriais relevantes.
- Estabelecer políticas e procedimentos para o tratamento adequado de informações pessoais, assegurando a privacidade dos indivíduos e o cumprimento das obrigações legais.

1.4 MOTIVAÇÃO, CONTRIBUIÇÃO E INOVAÇÃO

A implementação de um SGSI na EIB representa um desafio significativo. Embora existam muitos regulamentos e diretrizes disponíveis, adaptá-los à realidade específica de cada organização pode revelar-se uma tarefa complexa. A **motivação** para esta implementação é evidente, uma vez que a EIB tem sido proativa na implementação de sistemas integrados de gestão, como a ISO 9001 e a ISO 14001, mas priorizou os processos produtivos em detrimento da segurança dos sistemas de informação.

Além disso, a EIB está inserida num contexto de investimentos relacionados com a auto produção de energia e indústria 4.0, resultando na digitalização de processos e na utilização de componentes de Internet das Coisas (IoT), o que gera um aumento significativo na criação e armazenamento de informações. A implementação do SGSI **contribuirá** significativamente para a segurança desses sistemas, protegendo dados sensíveis e fortalecendo a confiança dos clientes, parceiros e stakeholders.

Esta iniciativa também está alinhada com os esforços recentes de inovação na EIB, que incluem visão artificial, rastreabilidade total de produtos e planos para a implementação de inteligência artificial. O SGSI abrirá caminho para a implementação segura de projetos de inovação, garantindo a confidencialidade, integridade e disponibilidade dos dados e consolidando a posição da EIB como líder **inovador** no seu setor.

1.5 METODOLOGIAS

Para executar este projeto de implementação de um SGSI, foram seguidos os seguintes passos:

1. **Levantamento do Estado de Arte e Revisão Bibliográfica:**
   Inicialmente, realizou-se um levantamento do estado de arte e uma revisão bibliográfica abrangente para compreender as melhores práticas e os requisitos relevantes em segurança da informação.

2. **Elaboração do Plano e Seleção de Normas e Frameworks:**
   Com base nas descobertas do levantamento inicial, elaborou-se um plano para a implementação do SGSI. Neste plano, foram selecionadas as normas e frameworks a serem seguidas, incluindo as normas da família ISO/IEC 27000 e a framework do NIST. Também foi considerada a conformidade com leis e regulamentos, como o RGPD.

3. **Implementação do SGSI:**
   O plano foi executado, e o SGSI foi implementado na organização, seguindo as normas e frameworks selecionadas e o ciclo PDCA comummente utilizado neste género de implementações.

4. **Gestão Documental:**
   A gestão documental foi melhorada, utilizando sinergias com outros sistemas de gestão em vigor para normalizar políticas e procedimentos. Foram identificados, classificados e revistos documentos, assegurando armazenamento adequado, gestão de versões, acesso e distribuição.

5. **Gestão de Riscos e Ativos:**
   A gestão de riscos e ativos foi realizada conforme a norma ISO/IEC 27005, com apoio na documentação do Centro Nacional de Cibersegurança (CNSC).

6. **Roadmap de Implementação:**
   Foi seguido o *roadmap* de Implementação do SGSI da Integrity demonstrado na figura 1, garantindo a implementação e adoção dos requisitos, políticas, procedimentos, controlos e práticas estabelecidos pela norma ISO/IEC 27001, adaptados ao âmbito e à realidade tecnológica e organizacional da EIB.

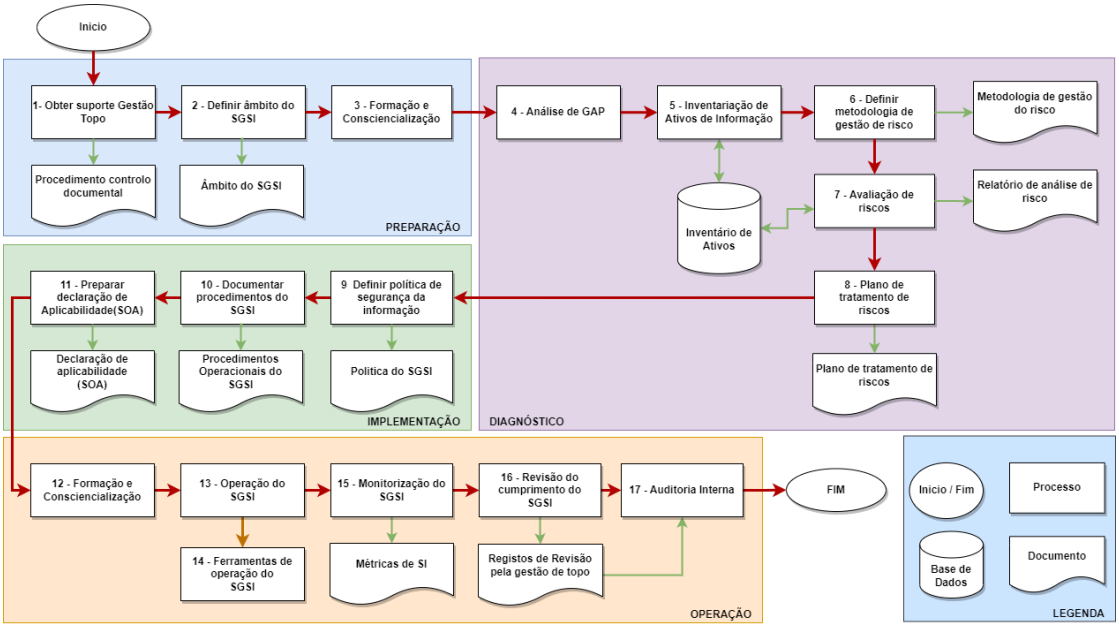


Figura 1: Roadmap de Implementação SGSI adaptado de Integrity, 2023

Estas etapas foram planeadas e executadas para garantir uma implementação sólida e consistente do SGSI na EIB, fornecendo um conjunto robusto de diretrizes e requisitos que abrangem todas as áreas relevantes da segurança da informação.

1.6 RESULTADOS ESPERADOS

A EIB tem feito um esforço considerável para criar infraestruturas físicas e lógicas que suportem os seus sistemas de Informação. No entanto, é preocupante que essas estruturas possam ser comprometidas devido a falhas na cibersegurança. A implementação deste projeto visa estabelecer um SGSI robusto e resiliente na empresa que será capaz de responder de forma organizada e rápida a eventos de segurança da informação, reduzindo os custos e impactos que tais eventos podem causar na estrutura da empresa e na confiança dos seus clientes.

Com a transição digital em curso, é reconhecido o papel crucial dos sistemas de informação, espera-se que o SGSI ajude a EIB a enfrentar com sucesso novos desafios associados a essa transição. Este permitirá a deteção antecipada de ameaças, seja de origem

interna ou externa, e a implementação de planos para tratar situações anómalas, como falhas de serviços de comunicação, perda abrupta de um servidor, roubo de equipamentos ou até catástrofes naturais. Além de que facilitará o cumprimento dos requisitos legais e regulatórios.

O cenário atual mudou rapidamente como utilizamos os sistemas de informação. Vivemos numa era digital, onde os locais de trabalho são virtuais e acessíveis a partir de qualquer parte do mundo por meio dos mais diversos dispositivos. Isso traz riscos significativos de exposição de dados sensíveis. Este projeto visa sensibilizar todos os colaboradores para esses desafios, criando políticas e diretrizes que promovam o uso responsável e consciente dos sistemas de informação.

1.7 ESTRUTURA DO DOCUMENTO

Na implementação deste trabalho, apresenta-se a organização do documento e a síntese do conteúdo de cada capítulo, estruturado da seguinte forma:

No primeiro capítulo 1, são apresentados a introdução, as metodologias adotadas, os objetivos e os resultados esperados que motivaram a realização deste projeto de implementação do Sistema de Gestão de Segurança da Informação (SGSI).

No capítulo 2, é realizada uma revisão bibliográfica do SGSI, abrangendo leis, padrões e normas internacionais, com especial ênfase nas normas da família 27000, principalmente a ISO/IEC 27001. Além disso, são apresentados trabalhos relacionados com o tema de implementação de um SGSI.

O caso de uso é apresentado no capítulo 3, onde é introduzida a organização objeto de estudo e são abordados temas como a sua estrutura, sistemas de gestão já implementados, nomeadamente ISO 9001 e 14001 e componentes tecnológicos utilizados.

O Capítulo 4, dedica-se à implementação do SGSI, onde se define o âmbito do SGSI, atribuem-se responsabilidades e cargos, realiza-se uma análise SWOT e GAP e definem-se as políticas, procedimentos e políticas de uso aceitável desenvolvidas no âmbito deste projeto. Por último concluí-se com a apresentação da declaração de aplicabilidade SoA.

No capítulo 5, é abordada a gestão de riscos. Neste capítulo, são realizadas atividades relacionadas com a gestão de ativos, incluindo a sua inventariação, classificação e

valorização. Além disso, é definida a metodologia de avaliação e análise de riscos, que resulta na elaboração de uma matriz de riscos e oportunidades, bem como num plano de tratamento de riscos. O capítulo conclui com a apresentação de um caso de uso.

O Capítulo 4.9, define as políticas, procedimentos e políticas de uso aceitável definidos no âmbito deste projeto. É dado ênfase à política geral do SGSI documento primordial na implementação de um SGSI.

A avaliação, monitorização e melhoria contínua do SGSI são apresentados no capítulo 6. Neste capitulo abordam-se temas como auditorias, comunicação, formação e consciencialização de todos os intervenientes e revisão do SGSI.

Por último, o capítulo 7 apresenta as conclusões relevantes para o desenvolvimento deste projeto, abordando analise critica, considerações e sugestão para trabalhos futuros.

2

REVISÃO BIBLIOGRÁFICA

Para assegurar a eficácia e a conformidade na implementação de um Sistema de Gestão de Segurança da Informação (SGSI), é de suma importância adquirir conhecimento e aplicar normas, frameworks, leis e trabalhos relacionados com o tema. Neste contexto, será apresentada uma visão abrangente dessas referências normativas e regulatórias, abordando as principais diretrizes e práticas recomendadas para uma implementação consistente e bem-sucedida de um SGSI.

2.1 SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO (SGSI)

Segundo Smulders. et al. (2018) na implementação de um SGSI a organização formula uma estrutura de controlo, essa estrutura fornece uma classificação lógica de todas as questões relacionadas com a segurança da informação, organizada por domínios. Um domínio é um grupo de assuntos que estão logicamente ligados, formando a base para a estrutura do SGSI, no entanto, alguns desses domínios possuem os próprios documentos de políticas, procedimentos e instruções de trabalho.

Os requisitos estabelecidos na norma ISO/IEC 27001 são de natureza genérica e aplicáveis a todas as organizações, independentemente do seu tipo, tamanho ou setor de atividade, sendo fundamental que uma organização não exclua nenhum dos requisitos especificados nas **cláusulas de 4 a 10** ao visar a conformidade com a norma. Na prática, significa que, durante o processo de certificação ISO/IEC 27001, a organização será auditada relativamente aos requisitos detalhados nas cláusulas de 4 a 10, estando esta abordagem alinhada com o processo de Gestão de Serviços de TI descrito na norma ISO/IEC 20000 (Smulders. et al., 2018).

Em suma a implementação de um SGSI é um processo contínuo, o qual a organização deve estar comprometida com a segurança da informação e procurar melhorias cons-

tantes. A norma ISO/IEC 27001 fornece orientações sobre cada etapa do processo de implementação que podem ser resumidas da seguinte forma:

1. **Compromisso da gestão de topo**
   Como evidenciado na **cláusula 5.1** da ISO/IEC 27001 a gestão de topo deve demonstrar um compromisso claro com a segurança da informação, estabelecer uma política de segurança e assegurar os recursos necessários e requisitos para implementar o SGSI.

2. **Definição do âmbito**
   É necessário estabelecer o âmbito do SGSI, identificando os ativos de informação relevantes, as partes interessadas envolvidas e os limites organizacionais.**Cláusula 4.3** da ISO/IEC 27001.

3. **Avaliação de riscos**
   Realizar uma análise de riscos para identificar ameaças, vulnerabilidades e potenciais impactos com segurança da informação, o que envolve a identificação dos ativos de informação, a avaliação das ameaças e vulnerabilidades, e a determinação dos riscos associados.**Cláusulas 6.1, 8.2 e 8.3** da ISO/IEC 27001.

4. **Seleção de controlos de segurança**
   Com base na análise de riscos, selecionar os controlos de segurança apropriados para mitigar os riscos identificados. Os controlos podem incluir políticas, procedimentos, tecnologias e medidas organizacionais.**Cláusulas 6.1.2 e 6.1.3** da ISO/IEC 27001.

5. **Implementação dos controlos**
   Implementar os controlos de segurança selecionados conforme as diretrizes estabelecidas na norma ISO/IEC 27001, pode envolver a criação de políticas e procedimentos, a implementação de tecnologias de segurança, a realização de formações e a consciencialização dos colaboradores. **Cláusula 8.1** da ISO/IEC 27001.

6. **Monitorização e avaliação**
   Estabelecer um sistema de monitorização contínua para verificar a eficácia dos controlos de segurança implementados, inclui auditorias internas, revisões periódicas, análise de incidentes de segurança e medição de indicadores de desempenho. **Cláusula 9** da ISO/IEC 27001.

7. **Melhoria contínua**
   Identificar oportunidades de melhoria e implementar ações corretivas para aprimorar o SGSI, Aprendendo com incidentes de segurança, revendo políticas e procedimentos, atualizando controlos de segurança, entre outras ações.**Cláusula 10** da ISO/IEC 27001.

Na figura 2 é apresentado um resumo das diferentes etapas e processos envolvidos na implementação da norma ISO/IEC 27001, os quais estão alinhados com o ciclo PDCA (Plan-Do-Check-Act).

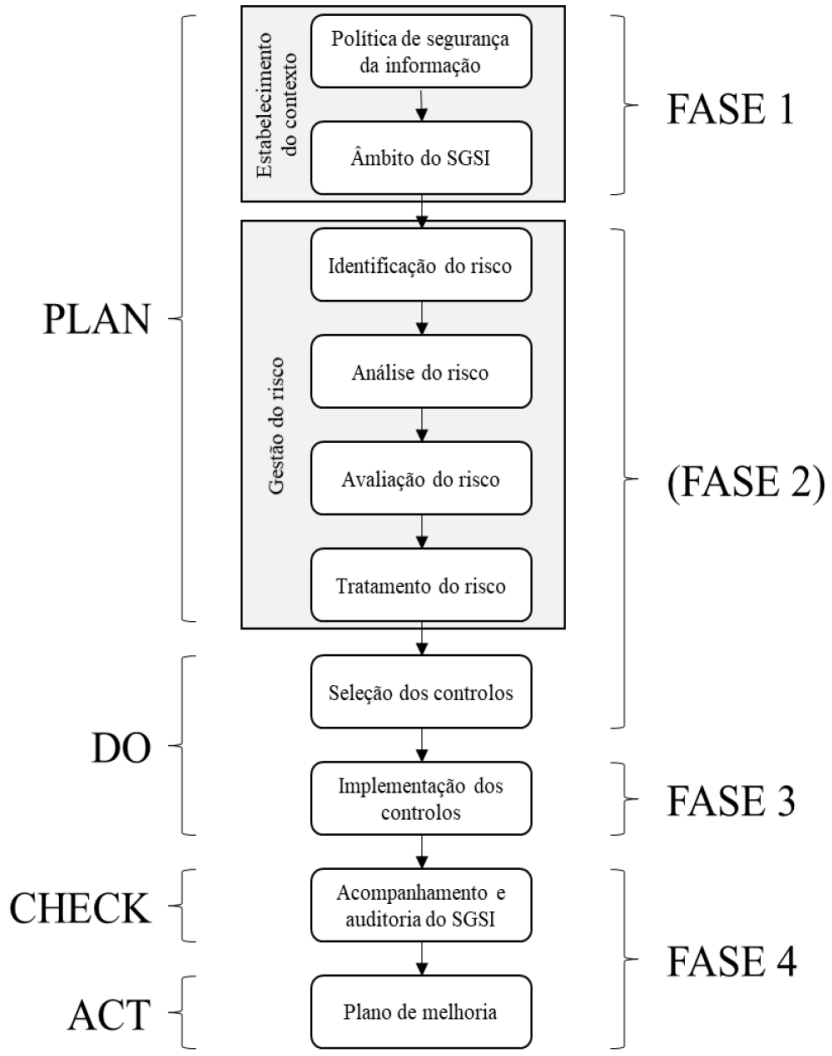


Figura 2: Processo Implementação SGSI Ferreira, 2020

2.1.1 *Impacto da certificação ISO/IEC 27001*

Segundo Ferreira (2020) antes de implementar um Sistema de Gestão de Segurança da Informação (SGSI) baseado na norma ISO/IEC 27001, é crucial que os decisores e investidores estejam cientes de que os benefícios operacionais e de negócio vão superar os inconvenientes. Para isso, é importante ter uma noção clara das vantagens e desvantagens da implementação deste tipo de padrão.

Entre as principais desvantagens da implementação, destacam-se as quantidades elevadas de recursos financeiros, esforço e tempo necessários, além do grande número de requisitos exigidos pela norma. Esses fatores podem afastar algumas organizações, levando-as a adiar a decisão de adotar um SGSI ou a optar por fazê-lo por meio de normas mais leves (Everett, 2011).

No entanto, há dois tipos de benefícios que podem ser obtidos com a adoção da norma: benefícios internos e externos. Os primeiros referem-se a melhorias nos procedimentos que podem resultar em reduções nos custos derivados da simplificação de processos e no número de incidentes relacionados com a segurança da informação. Os benefícios externos, por sua vez, determinam melhorias de mercado e nas relações com os clientes, que resultam da imagem transmitida de que a organização está preocupada com a segurança da informação (Hsu et al., 2016).

Embora haja escassez de estudos sobre o impacto da certificação ISO/IEC 27001 no desempenho das organizações, alguns estudos têm resultados contraditórios. Por exemplo, o estudo realizado por (Hudson e Orviska, 2013) verificou que organizações certificadas conseguem alcançar a maioria dos seus objetivos e identificaram quatro perspetivas em que é possível verificar esse impacto positivo:

- Financeira
  Apesar do aumento de alguns custos, a adoção destes standards trouxe benefícios financeiros globais às organizações que os adotaram.
- Clientes
  A demonstração de credibilidade e confiança na proteção das informações dos clientes aumentou a sua satisfação.

- Interna
  Verificaram-se melhorias em processos críticos para as organizações, como gestão de alterações, gestão de incidentes e gestão de ativos.
- Crescimento e aprendizagem
  A certificação permitiu não só o aumento de oportunidades para as organizações, mas também aliviou o trabalho dos funcionários através da utilização de procedimentos e métodos pré-definidos e bem compreendidos.

Por outro lado, o estudo de(Hsu et al., 2016) constatou que a certificação ISO/IEC 27001 não resulta num melhor desempenho financeiro, mas pode trazer satisfação em outros campos.

Uma justificação para esses resultados divergentes pode ser encontrada no estudo de (Hudson e Orviska, 2013) que mostra existirem diversos fatores externos capazes de aumentar ou diminuir a probabilidade desses padrões terem um impacto positivo no desempenho da organização. Por exemplo, organizações exportadoras ou sediadas em grandes cidades tendem a obter melhores resultados do que as não exportadoras ou localizadas em zonas rurais.

Em síntese, os efeitos da certificação ISO/IEC 27001 no desempenho das organizações podem assumir diferentes formas, dependendo de variáveis externas não controláveis. Embora possa não ter um impacto significativo no desempenho financeiro, as organizações tendem a sentir-se mais confiantes na sua relação com os clientes e mais seguras ao adotar processos normalizados. A certificação proporciona uma sensação de segurança e estabelece uma base sólida para uma gestão eficiente da segurança da informação.

2.1.2 *Vantagem competitiva*

Com a globalização, cada vez mais empresas estão a implementar padrões e normas internacionais para atender às expectativas dos seus clientes e especialmente, para resolver problemas emergentes dentro das próprias organizações. Estes padrões reduzem a variabilidade de desempenho entre fornecedores e promovem o comércio global. De acordo com Su. et al. (2015), a adoção destes standards é um fator decisivo na obtenção de uma vantagem competitiva.

Embora o estudo de Su. et al. (2015) seja referente às normas ISO 9001 e ISO 14001, as mesmas ideologias aplicam-se à norma ISO/IEC 27001 na continuidade do negócio e na melhoria contínua.

É expectável que as empresas que confiam a sua propriedade intelectual a outras empresas procurem salvaguardar as suas informações, o que torna a obtenção da certificação ISO/IEC 27001, uma vantagem competitiva clara, relativamente à concorrência. Ao aderir a esta norma, demonstra-se um compromisso sólido com a proteção e segurança dos dados, o que gera confiança por parte dos clientes e parceiros. Esta confiança na capacidade de proteger informações sensíveis cria uma reputação sólida e aumenta a atratividade e confiabilidade da empresa no mercado. Além da conformidade com os requisitos rigorosos da ISO/IEC 27001 ajudarem a mitigar riscos e a assegurar a conformidade regulamentar, promovem a confiança e tranquilidade dos intervenientes.

2.1.3 *Áreas de segurança da informação*

Conforme Zúquete (2018), a segurança de sistemas computacionais engloba três áreas de atividade essenciais, todas com especificidades próprias; defesa contra catástrofes físicas, defesa contra faltas/falhas previsíveis e defesa contra atividades não autorizadas:

- **A defesa contra catástrofes físicas**
  Garantir a sobrevivência de um sistema de informação ou serviço diante de eventos catastróficos que possam causar danos físicos. Exemplos desses eventos incluem catástrofes ambientais como terramotos, incêndios, inundações e quedas de raios, assim como catástrofes políticas tais como ataques terroristas e motins. Também é considerada a proteção contra catástrofes materiais, como a perda ou roubo de equipamentos computacionais, como discos magnéticos e computadores portáteis.
- **A defesa contra faltas/falhas previsíveis**
  Minimizar o impacto de eventos imprevistos, mas geralmente previsíveis. Embora o momento e a gravidade desses eventos sejam incertos, é possível identificá-los antecipadamente, sendo exemplo as falhas temporárias de conectividade em segmentos de rede e interrupções no fornecimento de energia elétrica ou de internet.

- **A Defesa contra atividades não autorizadas**
  Proteger os sistemas de informação contra ações deliberadas de indivíduos que procuram corromper ou subverter os sistemas computacionais, sendo exemplo o acesso não autorizado a informações confidenciais, alteração de dados sem permissão, entre outras iniciativas maliciosas.

2.1.4 *Políticas e procedimentos de segurança da informação*

A ISO/IEC 27000 define política como "as intenções e direção de uma organização, formalmente aceite pela gestão de topo". e procedimento como "um conjunto de atividades inter-relacionadas ou em interação que transforma inputs em outputs". Já um procedimento define-se como um método específico de executar uma atividade ou processo, desta forma, serão elaborados documentos para cada controlo de segurança.

As políticas de segurança da informação têm como principal objetivo proteger as informações sensíveis da organização contra ameaças internas e externas, garantindo a confidencialidade, integridade e disponibilidade dessas informações. Estas políticas são implementadas para estabelecer diretrizes claras de segurança que devem ser seguidas por todos os colaboradores da organização, a fim de prevenir incidentes de segurança da informação, minimizar riscos e evitar prejuízos financeiros e de reputação para a organização.

Além disso, as políticas de segurança da informação visam cumprir as obrigações legais e regulatórias aplicáveis à proteção de informações sensíveis, promover uma cultura de segurança da informação na organização, garantir a continuidade dos negócios em caso de incidentes de segurança e aumentar a confiança dos clientes e parceiros da empresa.

2.1.5 *Gestão de riscos*

Segundo o Centro Nacional de Cibersegurança a gestão de riscos é um processo estruturado no qual a organização identifica potenciais ameaças que podem explorar vulnerabilidades dos ativos, avaliando os níveis de risco associados, durante esse processo, são analisadas as probabilidades de ocorrência dessas ameaças e os possíveis impactos resultantes.

2.1.5.1 *Termos e definições*

Com o intuito de promover uma melhor compreensão dos termos utilizados na gestão de riscos, serão apresentados de seguida alguns dos conceitos frequentemente utilizados tendo como origem as definições do Centro Nacional de Cibersegurança, 2023:

- **Ameaça**
  Potencial causa de um incidente indesejado, que pode provocar danos a um sistema, indivíduo ou organização.
- **Ativo**
  Todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos considerados essenciais, geridos ou detidos pela entidade, que suportam, direta ou indiretamente, um ou mais serviços.
- **Vulnerabilidade**
  Fraqueza de um ativo ou controlo que pode ser explorada por uma ou mais ameaças.
- **Impacto**
  Refere-se às consequências resultantes da ocorrência de um determinado evento de segurança em um ou mais recursos, o qual geralmente resulta em efeitos diretos ou indiretos para os recursos mencionados.
- **Risco**
  Uma circunstância ou um evento razoavelmente identificável, com um efeito potencial adverso na segurança das redes e dos sistemas de informação.
- **Evento**
  Ocorrência ou alteração de um conjunto particular de circunstâncias;
- **Incidente**
  Um evento com um efeito adverso real na segurança das redes e dos sistemas de informação.

2.2 LEIS E REGULAMENTOS

Em Portugal, existem várias leis e regulamentos que regulamentam a segurança cibernética e a proteção de dados.

A seguir serão apresentadas as leis e regulamentos mais comuns que se inserem no âmbito deste trabalho e que regulam a cibersegurança e a proteção de dados em Portugal. A definição e elaboração destas leis é supervisionada por diversas entidades, incluindo o Centro Nacional de Cibersegurança, a Comissão Nacional de Proteção de Dados e outras autoridades competentes.

2.2.1 *Lei do Cibercrime - Lei n.º 109/2009*

Lei do Cibercrime, também conhecida como Lei n.º 109/2009, é uma legislação em Portugal cujo objetivo é combater os crimes cometidos em ambiente digital. Esta lei estabelece um conjunto de normas e sanções para lidar com atividades ilícitas relacionadas com as tecnologias de informação e comunicação.

A Lei do Cibercrime abrange uma ampla gama de delitos, tais como acesso ilegal a sistemas informáticos, sabotagem informática, falsificação informática, pornografia infantil, fraude eletrónica, entre outros. Estabelece as penalidades a serem aplicadas aos infratores desses crimes e define as responsabilidades dos envolvidos.

Prevê medidas de cooperação internacional para facilitar a investigação e a repressão desses crimes, garantindo assim a segurança e a integridade das informações e sistemas digitais. Desempenha um papel crucial na proteção da sociedade e na promoção da justiça no contexto digital (*Lei do Cibercrime* 2009).

2.2.2 *Segurança das Redes e de toda a informação - Lei n.º 46/2018*

A Lei n.º 46/2018, conhecida como "Segurança das Redes e de toda a Informação", visa estabelecer as medidas e procedimentos necessários para garantir a segurança das redes

e da informação em Portugal, é baseada em diretrizes e normas da União Europeia relacionadas com a cibersegurança.

Abrange diversas áreas, incluindo a proteção de infraestruturas críticas, a prevenção de incidentes de segurança, a gestão de riscos e a cooperação entre entidades públicas e privadas. Estabelece requisitos e responsabilidades para os operadores de serviços essenciais, fornecedores de serviços digitais e outras entidades relevantes.

A Lei n.º 46/2018 prevê a criação de um regime sancionatório, estabelecendo as infrações e as correspondentes coimas para quem não cumprir com as obrigações de segurança estabelecidas. A Autoridade Nacional de Segurança Cibernética (ANCS) é a entidade responsável pela supervisão e fiscalização do cumprimento desta lei.

É importante referir que a Lei nº 46/2018 visa fortalecer a cibersegurança em Portugal, promovendo a proteção das redes e da informação contra ameaças e ataques cibernéticos, contribui para a criação de um ambiente seguro e confiável das atividades digitais, tanto no setor público quanto no privado (*Lei n.º 46/2018* 2018).

2.2.3 *Decreto-Lei n.º 55/2019*

Decreto-Lei n.º 55/2019 é uma legislação portuguesa que estabelece o regime jurídico da segurança do ciberespaço, visando promover a proteção das redes e sistemas de informação em Portugal. Foi criado como uma medida para fortalecer a cibersegurança e combater as ameaças e os ataques cibernéticos que podem afetar organizações e indivíduos.

Este decreto-lei define as obrigações e responsabilidades das entidades públicas e privadas no que diz respeito à segurança do ciberespaço. Estabelece a necessidade de implementação de medidas técnicas, organizacionais e jurídicas para prevenir, detetar e responder a incidentes de segurança cibernética.

O Decreto-Lei n.º 55/2019 está alinhado com a legislação europeia em matéria de cibersegurança, bem como com diretrizes e melhores práticas internacionais.

Algumas das principais áreas abordadas pelo Decreto-Lei n.º 55/2019 incluem:

- Definição de requisitos de segurança
  O decreto-lei estabelece os requisitos mínimos de segurança que as organizações devem adotar para proteger as suas redes e sistemas de informação.
- Identificação de operadores críticos
  São identificados os operadores de serviços essenciais, operadores de infraestruturas críticas e fornecedores de serviços digitais com obrigações específicas de segurança cibernética.
- Criação de um Centro Nacional de Cibersegurança
  O decreto-lei prevê a criação de um Centro Nacional de Cibersegurança para coordenar e promover a segurança cibernética em Portugal, bem como para monitorizar ameaças e incidentes de segurança.
- Notificação de incidentes
  Estabelece a obrigatoriedade de notificação de incidentes de segurança cibernética às autoridades competentes, visando uma resposta rápida e eficaz a esses incidentes.
- Regime sancionatório
  O decreto-lei estabelece sanções administrativas e coimas para o não cumprimento das obrigações de segurança cibernética.

(*Decreto-Lei n.º 55/2019* 2019)

2.2.4 *Regulamento Geral sobre a Proteção de Dados - RGPD*

RGPD (Regulamento Geral sobre a Proteção de Dados) é aplicado através da Lei n.º 58/2019, que assegura a execução do RGPD no ordenamento jurídico português. O RGPD é uma regulamentação da União Europeia que estabelece as regras sobre a proteção de dados pessoais e a privacidade dos indivíduos.

A versão portuguesa do RGPD incorpora as disposições do regulamento europeu e adapta-as à legislação nacional. Define os princípios, direitos e obrigações relacionados com o tratamento de dados pessoais em Portugal. Alguns dos principais pontos abordados pelo RGPD Português incluem:

- **Definição de conceitos**
  O RGPD define os termos e conceitos relacionados com a proteção de dados, como dados pessoais, tratamento de dados, responsáveis pelo tratamento, subcontratantes, entre outros.
- **Princípios de proteção de dados**
  Estabelece os princípios que devem ser observados no tratamento de dados pessoais, tais como o princípio da licitude, lealdade e transparência; o princípio da limitação da finalidade; o princípio da minimização dos dados; o princípio da exatidão; o princípio da limitação da conservação; o princípio da integridade e confidencialidade; e o princípio da responsabilidade.
- **Direitos dos titulares dos dados**
  Define os direitos dos indivíduos em relação aos seus dados pessoais, como o direito de acesso, retificação, eliminação, oposição e portabilidade.
- **Obrigações dos responsáveis pelo tratamento**
  Estabelece as responsabilidades dos responsáveis pelo tratamento de dados pessoais, incluindo a adoção de medidas técnicas e organizacionais adequadas para garantir a segurança dos dados.
- **Transferências internacionais de dados**
  Regula as transferências de dados pessoais para países fora da União Europeia, garantindo que essas transferências sejam feitas conforme os requisitos de proteção de dados.
- **Autoridade de controlo**
  Estabelece a Comissão Nacional de Proteção de Dados (CNPD) como a autoridade de controlo em Portugal, responsável pela supervisão e aplicação das normas de proteção de dados.

O RGPD é fundamental para garantir a proteção dos direitos dos indivíduos em relação aos seus dados pessoais, promovendo a transparência e a segurança no tratamento desses dados (*Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho* 2016).

2.3 NORMAS

Nesta secção serão apresentadas as normas consideradas importantes para a realização deste projeto ou porque já fazem parte dos sistemas de gestão da organização utilizada com caso de estudo ou porque são importantes para se entender a evolução e dependência que têm com as normas aplicáveis a sistemas de segurança da informação.

2.3.1 *NP EN ISO 9001*

A NP EN ISO 9001:20015 é a norma portuguesa transcrita da norma internacional ISO 9001:2015 que define os requisitos para um sistema de gestão da qualidade (SGQ) das organizações. Pretende garantir que as empresas fornecem produtos e serviços consistentes e de alta qualidade que atendem às necessidades dos clientes e regulamentos aplicáveis. Esta norma fornece uma estrutura para ajudar as organizações a aperfeiçoarem os seus processos de modo a ficarem mais eficientes, além de aumentar a satisfação dos clientes através da implementação efetiva do SGQ, incluindo processos de melhoria contínua. A certificação ISO 9001 é concedida após uma avaliação rigorosa por uma entidade de certificação independente, e serve como prova do comprometimento da empresa com a excelência em gestão da qualidade (Oliveira, 2015).

A norma ISO 9001 foi publicada pela primeira vez em 1987, baseada na British Standard BS 5750. Em 2000, houve uma revisão da norma ISO 9001, resultando no reforço da importância dos clientes e da melhoria contínua, e no incentivo à adoção de uma abordagem por processos. Em 2008, houve mais uma revisão da norma ISO 9001:2000, resultando na publicação da ISO 9001:2008. Por último, em 2015 é lançada uma versão atualizada da ISO 9001:2008, de onde resulta a versão Portuguesa NP EN ISO 9001:2015 onde são evidenciadas diferenças significativas (Oliveira, 2015):

- Pensamento baseado em risco: A ISO 9001:2015 adota uma abordagem baseada em risco para garantir que a gestão da qualidade esteja alinhada às necessidades do negócio e às expectativas dos clientes.

- Liderança: A nova versão enfatiza a importância da gestão de topo na definição e implementação do sistema de gestão da qualidade.
- Gestão de processos: A ISO 9001:2015 destaca a importância de uma abordagem centrada em processos para garantir a eficiência e a eficácia do sistema de gestão da qualidade.
- Integração com outros sistemas de gestão: A nova norma incentiva a integração do sistema de gestão da qualidade com outros sistemas de gestão, como o **ambiental**[1] e o de **segurança da informação**.
- Melhoria contínua: A ISO 9001:2015 enfatiza ainda mais a necessidade de uma abordagem de melhoria contínua para garantir a evolução constante do sistema de gestão da qualidade.

Em resumo, a ISO 9001:2015 é uma norma mais moderna e adaptada às necessidades atuais da gestão da qualidade, enquanto a ISO 9001:2008 é a versão anterior com uma abordagem mais simplificada e menos abrangente.

2.3.1.1 *Abordagem por processos*

A Norma promove a adoção de uma abordagem por processos na gestão da qualidade para aumentar a satisfação do cliente e atender aos seus requisitos. A abordagem por processos envolve a gestão sistemática dos processos e as suas interações para atingir os resultados desejados, utilizando o ciclo PDCA e o pensamento baseado em risco. A aplicação da abordagem por processos resulta em compreensão e satisfação dos requisitos, processos avaliados em termos de valor, desempenho eficaz dos processos e melhoria baseada na avaliação de dados. A Figura 3 mostra a interação entre os elementos de um processo e os pontos de monitorização e medição necessários para o controlo (*NP ISO 9001* 2015).

1 Certificação ISO 14001:2015 que a EIB possui

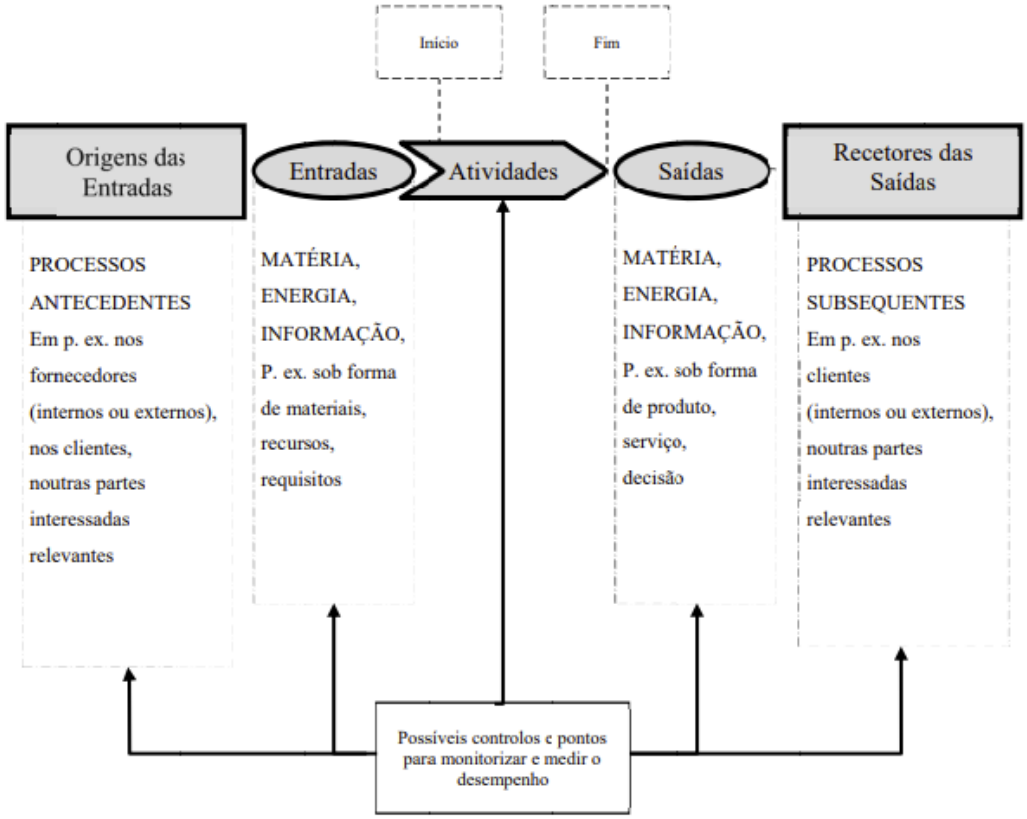


Figura 3: Representação esquemática, elementos de um processo simples (*NP ISO 9001* 2015)

2.3.1.2 *Ciclo PDCA*

Segundo *NP ISO 9001* (2015) O ciclo PDCA pode ser aplicado a todos os processos e ao sistema de gestão da qualidade como um todo. A Figura 4 representa como podem ser agrupadas as secções 4 a 10 por referência ao ciclo PDCA. Este pode ser descrito resumidamente da seguinte forma:

- **Planear** (plan): estabelecer os objetivos do sistema e os seus processos, bem como os recursos necessários para obter resultados de acordo os requisitos do cliente e as políticas da organização e identificar e tratar riscos e oportunidades;
- **Executar** (do): implementar o que foi planeado;

- **Verificar** (check): monitorizar e (onde aplicável) medir os processos e os produtos e serviços resultantes por comparação com políticas, objetivos, requisitos e atividades planeadas e reportar os resultados;
- **Atuar** (act): empreender ações para melhorar o desempenho conforme necessário.

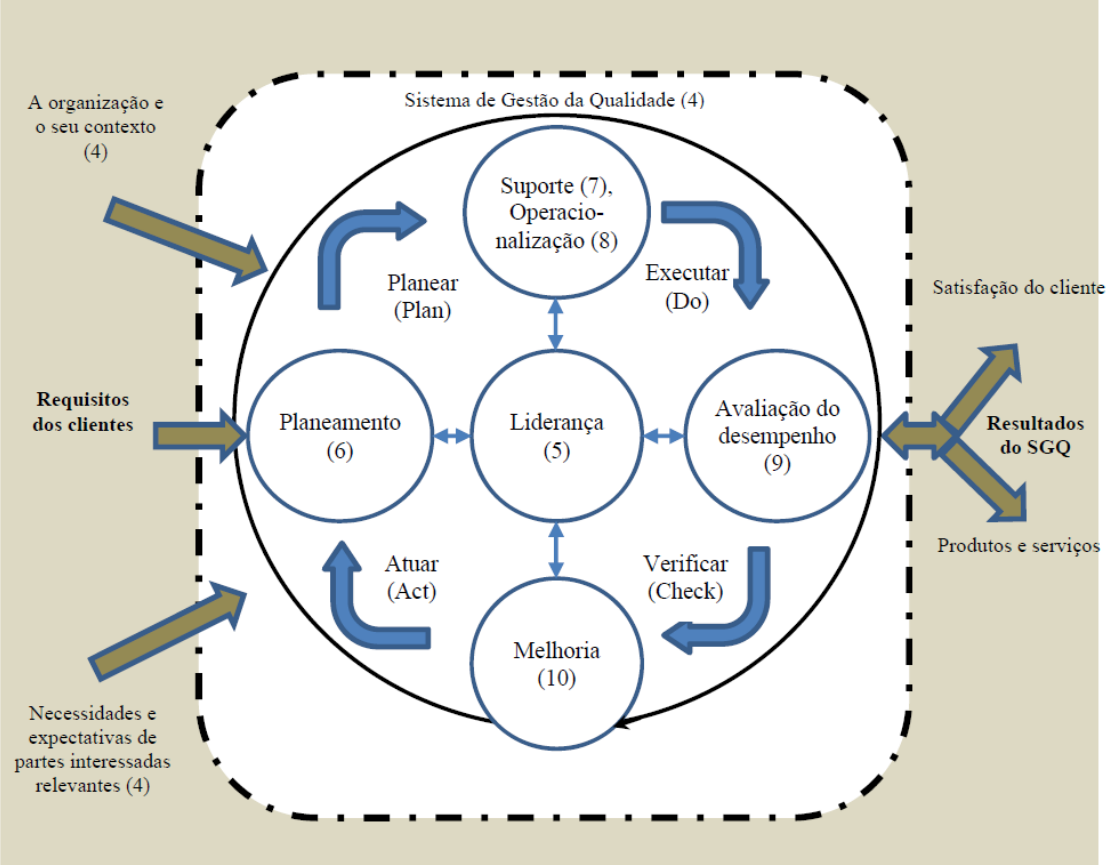


Figura 4: Representação da ISO 9001 no ciclo PDCA (*NP ISO 9001* 2015)

2.3.1.3 *Pensamento baseado em risco*

A norma exige ações preventivas para evitar não conformidades, análise de não conformidades e medidas para impedir a sua repetição. A organização deve planear e implementar ações para tratar os riscos e oportunidades para melhorar o desempenho do sistema de gestão da qualidade e evitar efeitos negativos. Podem surgir oportunidades de circunstâncias favoráveis que ajudem a atrair clientes, inovar, reduzir desperdício e melhorar a produtividade. Além disso, é importante considerar os riscos associados às oportunidades.

Risco é a consequência da incerteza e pode ter efeitos positivos ou negativos. Alguns riscos podem resultar em oportunidades, mas nem todos os efeitos positivos do risco resultam em oportunidades (*NP ISO 9001* 2015).

2.3.1.4 *Relacionamento com outras normas de sistemas de gestão*

A ISO 9001 não inclui requisitos específicos de outros sistemas de gestão, mas relaciona-se com a ISO 9000 (fornece os conceitos e princípios fundamentais de gestão de qualidade) e ISO 9004 (fornece orientações para melhorar o desempenho geral da organização). Apesar disso, segue a estrutura de alto nível definida pela ISO, conhecida como Anexo SL, o que facilita a integração de diferentes sistemas de gestão numa organização.

A Norma permite que uma organização utilize a abordagem por processos, combinada com o ciclo PDCA e considerando os riscos envolvidos, para alinhar ou integrar o seu próprio sistema de gestão da qualidade com os requisitos de outras normas de sistemas de gestão.

2.3.2 *NP EN ISO 14001*

A NP ISO 14001:2015 é a norma portuguesa transcrita da norma internacional ISO 14001:2015 que estabelece os requisitos para um sistema de gestão ambiental (SGA) eficaz. Concentra-se em ajudar as organizações a identificar e controlar os seus impactos ambientais e melhorar a sua eficiência ambiental.

A norma baseia-se no conceito de pensamento fundamentado em risco e exige que as organizações considerem tanto os riscos quanto as oportunidades ambientais. O objetivo é melhorar a eficiência do SGA, obter melhores resultados ambientais e prevenir efeitos negativos. Além disso, a ISO 14001 incentiva as organizações a considerarem o impacto ambiental ao longo de todo o ciclo de vida dos seus produtos e serviços. A implementação da norma é voluntária, mas as organizações que a adotam são reconhecidas como comprometidas com o meio ambiente (*NP ISO 14001* 2015).

2.3.3 *NP ISO 31000*

A NP ISO 31000:2012 é a norma portuguesa transcrita da norma internacional ISO 31000:2009 que estabelece princípios e diretrizes para gestão de riscos.

Fornece uma abordagem sistemática e estruturada para identificar, avaliar, gerir e comunicar riscos em qualquer área de uma organização, independentemente do seu tipo, além disso, ajuda as organizações a alcançarem os seus objetivos, sejam eles financeiros, operacionais ou de outra natureza, enquanto se protegem contra potenciais ameaças.

A norma concentra-se em fornecer ferramentas para desenvolver uma abordagem proativa e sistemática para gerir riscos e maximizar as oportunidades, é projetada para ser usada em conjunto com outras normas e regulamentos. Ajuda as organizações a alinhar e integrar a gestão de riscos em todo o seu domínio, operações, processos, funções e projetos (*NP ISO 31000* 2012). A figura 5 ilustra a estrutura, os princípios e os processos da gestão do risco.

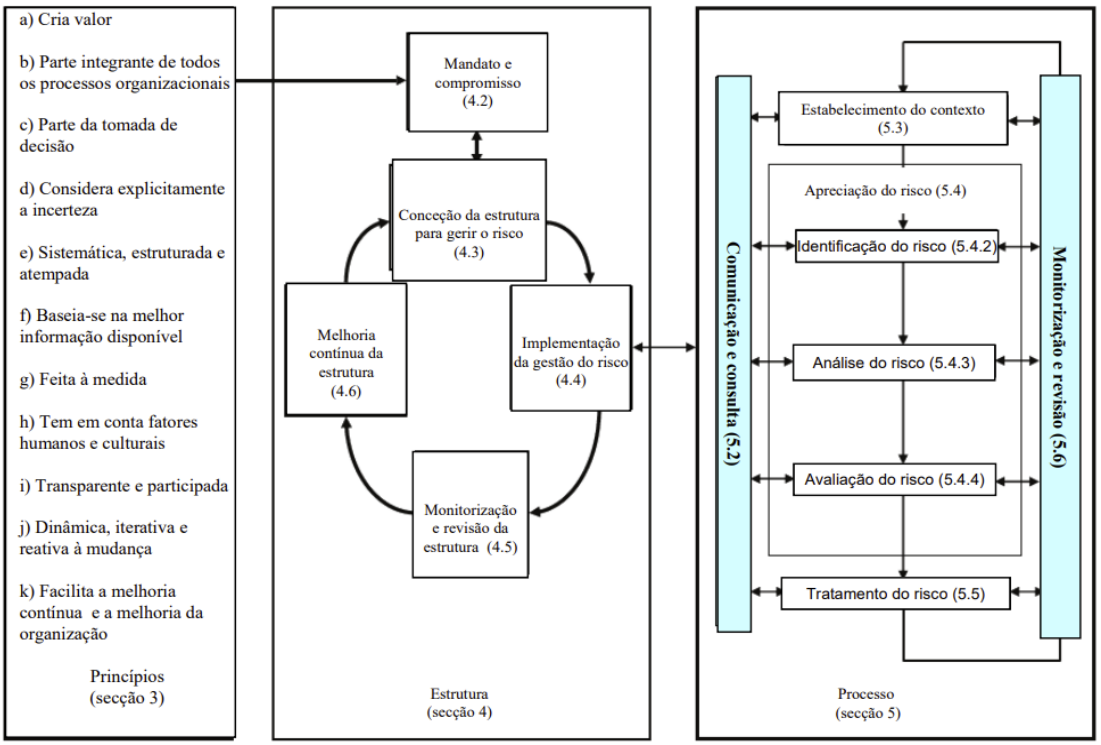


Figura 5: Relações entre princípios, estrutura e processo da gestão do risco (*NP ISO 31000* 2012)

Atualmente a norma ISO 31000 encontra-se na versão 2018, esta segunda edição cancela e substitui a primeira edição (ISO 31000:2009) que foi tecnicamente revista. As principais alterações relativamente à edição anterior são as seguintes:

- Revisão dos princípios da gestão do risco, critérios-chave para o seu sucesso;
- Destaque da liderança pela gestão de topo e da integração da gestão do risco, começando pela governança da organização;
- Maior ênfase na natureza iterativa da gestão do risco, tendo em conta que experiências, conhecimento e análises suplementares podem levar à revisão de elementos, ações e controlos em cada fase do processo;
- Otimização do conteúdo para maior foco na sustentação de um modelo de sistemas aberto para adequação a múltiplas necessidades e contextos.

A gestão do risco é baseada nos princípios, estrutura e processos descritos na figura 6. Estes componentes poderão já existir, total ou parcialmente na organização. No entanto, poderão ter de ser adaptados ou melhorados para que a gestão do risco seja eficiente, eficaz e consistente(*ISO 31000* 2018).

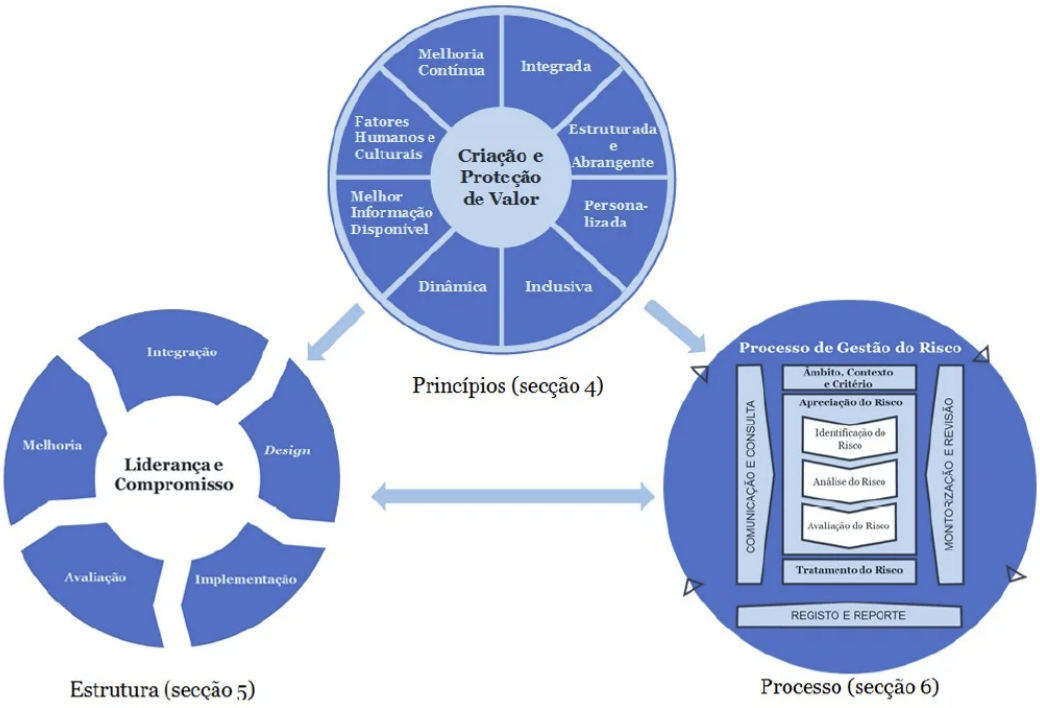


Figura 6: Princípios, estrutura e processo (*ISO 31000* 2018)

2.3.4 *ISO/IEC 27001*

ISO/IEC 27001 *"Information security, cybersecurity and privacy protection - Information security management systems - Requirements"*.

Standard internacional para sistemas de gestão de segurança de informação SGSI, vulgarmente conhecida com ISO 27001, foi projetada para fornecer controlos de segurança necessários para manter e melhorar continuamente os SGSI através da análise de risco. A sua primeira versão foi publicada em 2005 e teve como base a Norma britânica BS 7799-2 (*ISO/IEC 27001* 2013).

Seguramente uma das normas internacionais mais utilizada na gestão de sistemas da segurança da informação, tem como princípio geral a implementação de processos e controlos visando mitigar e gerir o risco da organização em relação à segurança da informação (Ramos, 2022).

De acordo com *ISO/IEC 27001* (2013), a norma não impõe requisitos específicos de segurança da informação, uma vez que os requisitos necessários podem variar conforme as particularidades das organizações, os controlos da ISO/IEC 27001 estão sumariados no Anexo A. Ao implementar a ISO/IEC 27001, as organizações podem selecionar os controlos aplicáveis aos riscos de informação que enfrentam, referindo-se aos listados no Anexo A e possivelmente complementando-os com opções adicionais, conhecidas como conjuntos de controlos estendidos.

Apesar da ligação entre esta norma e outras da série 27000, existe um alinhamento com a norma ISO 31000 Gestão do Risco - Princípios e linhas de orientação, pois esta apresenta os requisitos para a avaliação e tratamento de riscos de segurança da informação à medida das necessidades da organização. Dado que os requisitos definidos na norma ISO/IEC 27001 "são genéricos e aplicáveis a todas as organizações, independentemente do seu tipo, dimensão ou natureza" (*ISO/IEC 27001* 2013).

A ISO/IEC 27001 também pode ser utilizada por partes interessadas externas, nomeadamente por clientes que obrigam os seus fornecedores a implementar a norma, como garantia que a organização possui práticas eficazes de gestão da segurança da informação, nomeadamente dados financeiros, propriedade intelectual, dados de colaboradores e outras informações de clientes e parceiros(Ramos, 2022).

Acresce ainda referir que da família de normas ISO/IEC 27000 esta é a única norma, para a qual é possível, obter um certificado emitido por empresas acreditadas e autorizadas para o efeito (Ta-Seen, 2023).

2.3.4.1 *Ciclo PDCA*

A ISO/IEC 27001 considera a gestão da segurança da informação como um processo de gestão estruturado capaz de garantir requisitos de segurança para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar um SGSI. Promove ainda a adoção da abordagem por processos com base na utilização do modelo PDCA como ilustrado na figura 7.

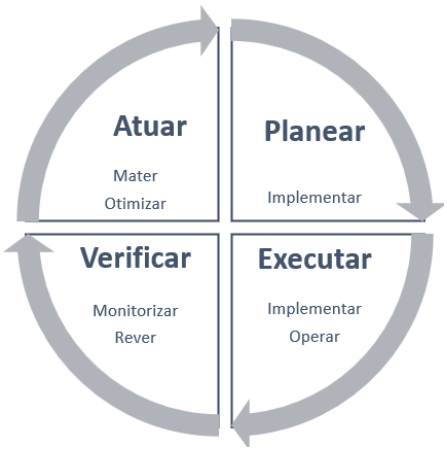


Figura 7: Processo iterativo PDCA para implementação de um SGSI

Segundo Carvalho e Marques (2019), o ciclo PDCA: (Plan - Do - Check - Act) é um ciclo de melhoria contínua que procura tornar os processos de gestão mais ágeis, claros e objetivos. No contexto da ISO/IEC 27007, o ciclo PDCA figura 7 consiste nas seguintes fases:

1. Planear - **Plan**
   Fase na qual o sistema de gestão de segurança da informação é estabelecido. Isso inclui a definição de objetivos, processos e procedimentos para gestão de riscos, projetar os controles a serem aplicados e a documentação a ser produzida.

2. Executar - **Do**

   Fase de implementação e operação do SGSI, com a aplicação prática dos controlos de segurança, processos e procedimentos estabelecidos.

3. Verificar - **Check**

   Fase na qual os indicadores de desempenho dos controlos implementados são avaliados e confrontados com a política do SGSI. Os resultados exigem análise crítica e revisão de políticas e procedimentos quando aplicável.

4. Atuar - **Act**

   Fase na qual são realizadas ações corretivas e preventivas nos controlos cujos indicadores de desempenho não apresentaram resultados satisfatórios, visando melhorar continuamente o SGSI.

2.3.4.2 *Componentes da ISO/IEC 27001*

A norma ISO/IEC 27001 é composta por duas componentes distintas (Integrity, 2023):

1. Na primeira componente estão definidas as regras e os requisitos de cumprimento da norma "A exclusão de quaisquer dos requisitos especificados nas secções de 4 a 10 não é aceitável para uma organização que reivindica a conformidade com esta norma." *ISO/IEC 27001* (2013). O diagrama da figura 8 apresenta os requisitos essenciais para a conformidade com a norma.

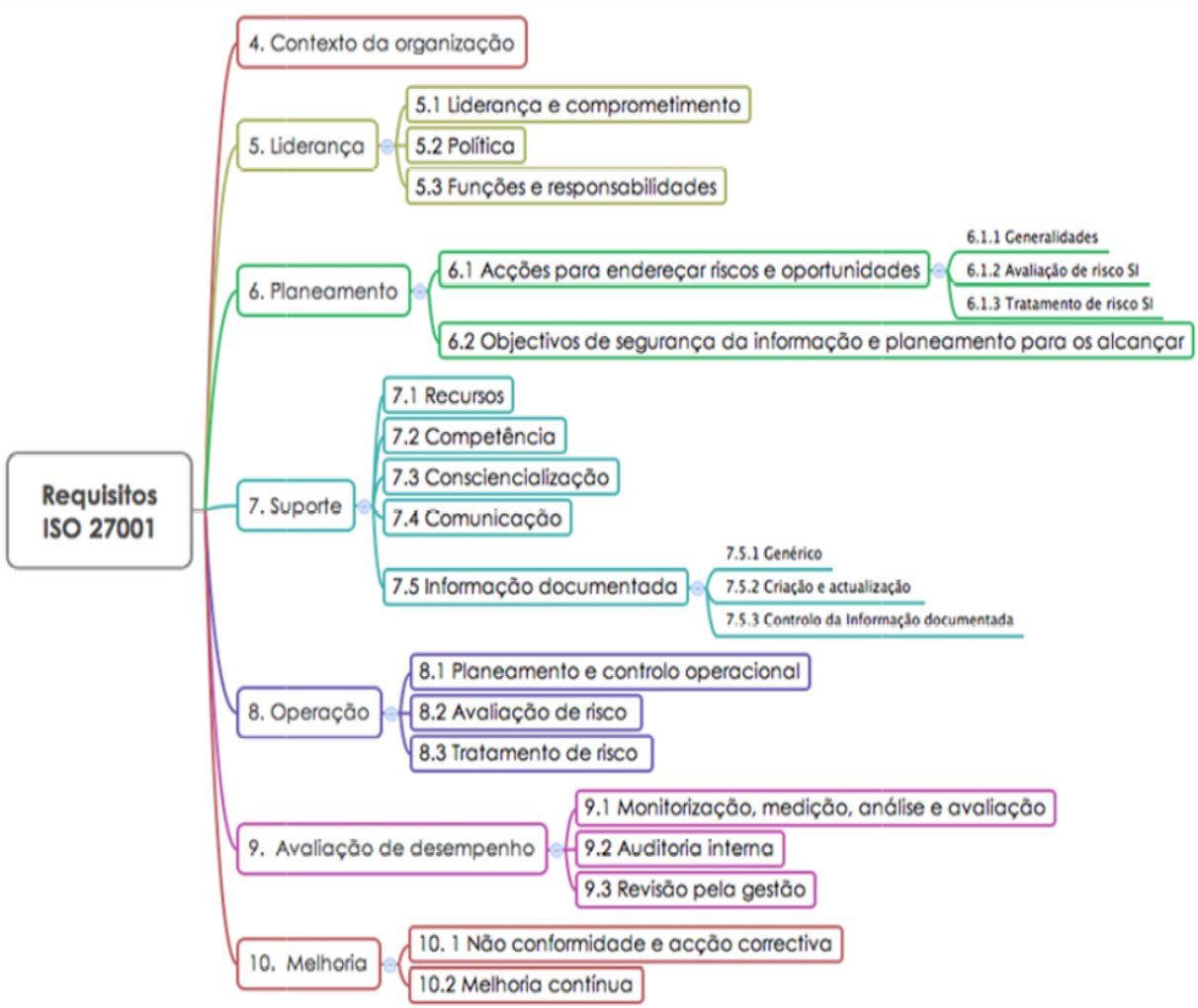


Figura 8: Requisitos da ISO/IEC 27001 adaptado de (Integrity, 2023)

A Figura 9 compila a aplicação do ciclo PDCA às cláusulas definidas na ISO/IEC 27001.

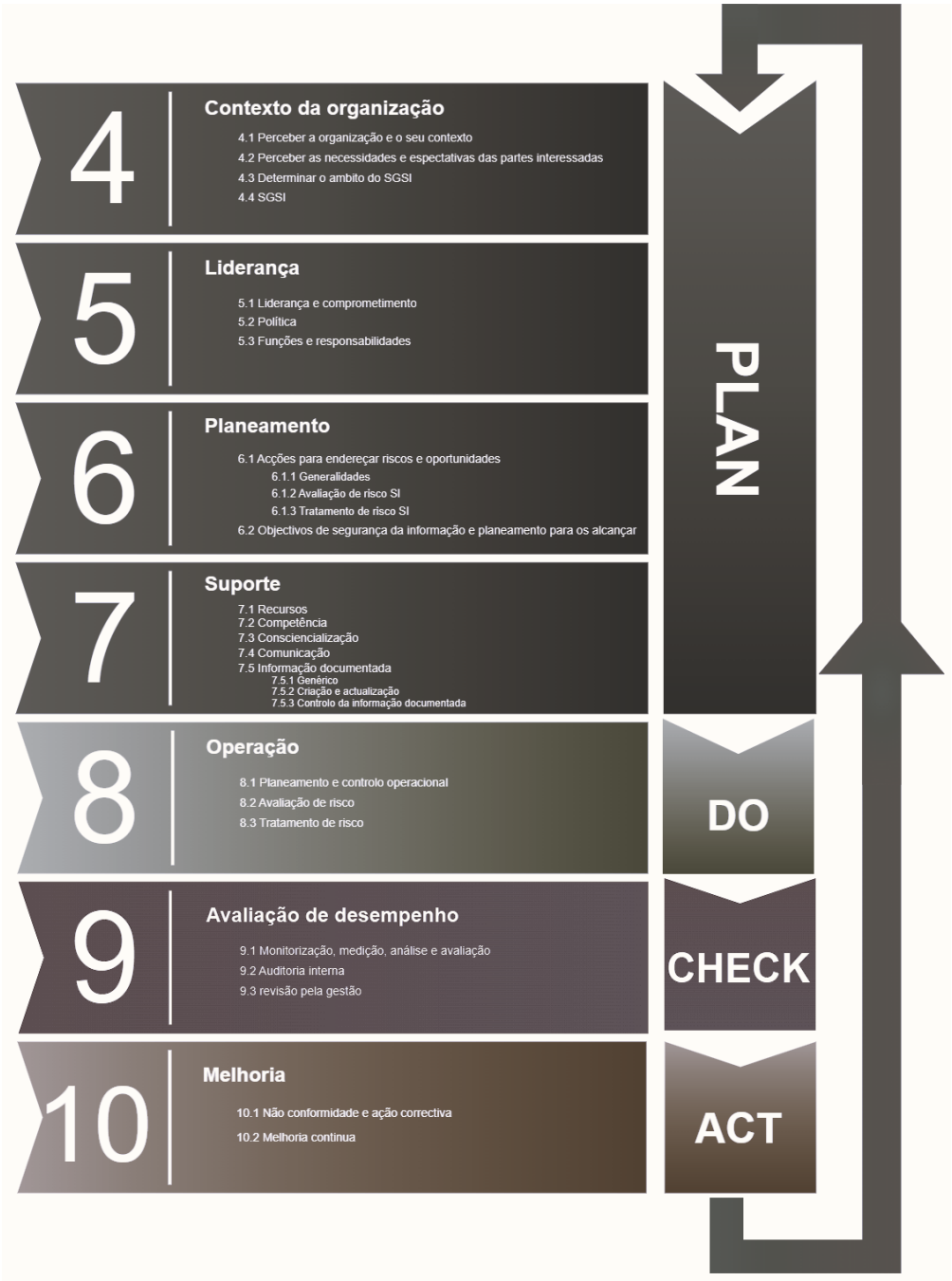


Figura 9: Ciclo PDCA aplicado às cláusulas da ISO/IEC 27001

2. Segunda componente, denominada Anexo A, especifica os objetivos de controlo e os controlos de A.5 a A.18. A figura 10 apresenta os controlos a adotar na norma.

   A *ISO/IEC 27001* (2013) refere na **cláusula 6.1.3** que os objetivos de controlo e controlos listados no Anexo A, não são exaustivos e podem ser necessários objetivos de controlo adicionais, ou seja, as organizações podem conceber controlos, conforme necessário.

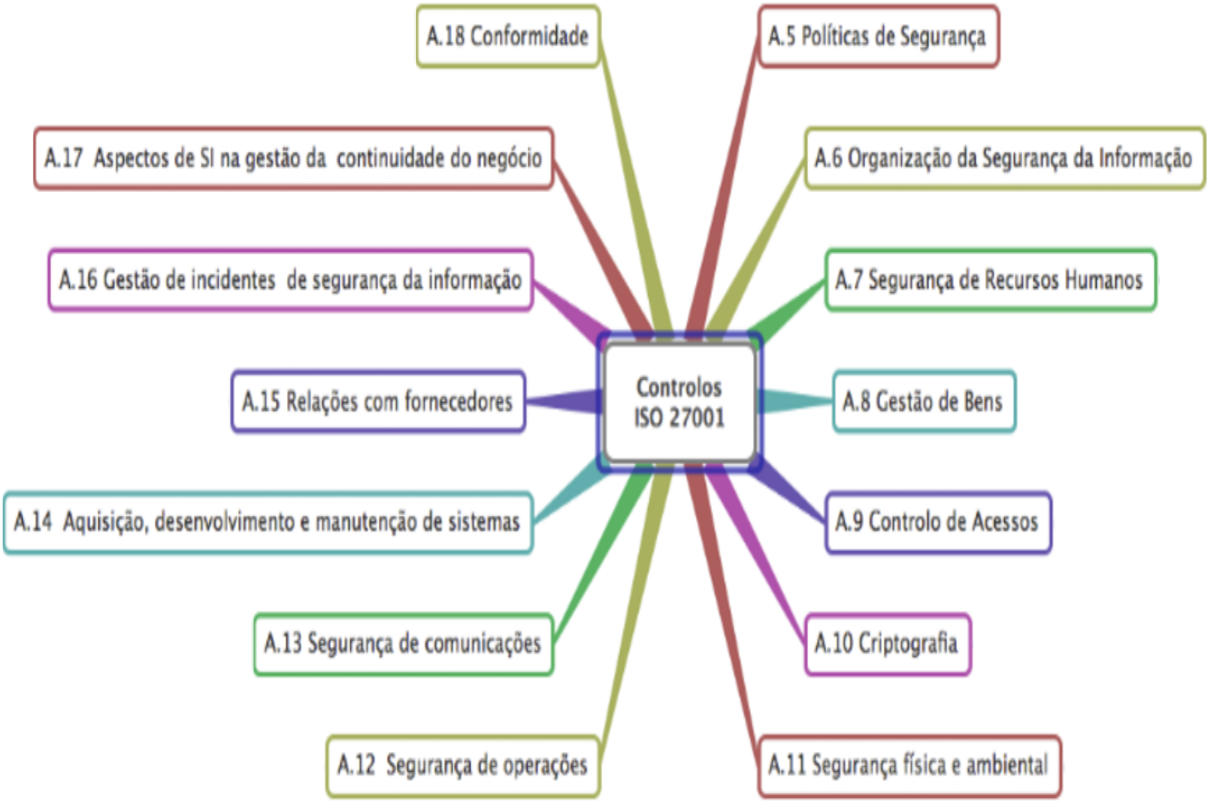


Figura 10: Controlos da ISO/IEC 27001 (Integrity, 2023)

Desta forma, a estrutura global da ISO/IEC 27001 pode ser apresentada como a figura 11 em que as cláusulas com os requisitos correspondentes ao ciclo de melhoria contínua estão representados no ciclo interior, as cláusulas com os requisitos gerais do SGSI no triângulo exterior e o anexo A com os objetivos de controlo no quadro a laranja.

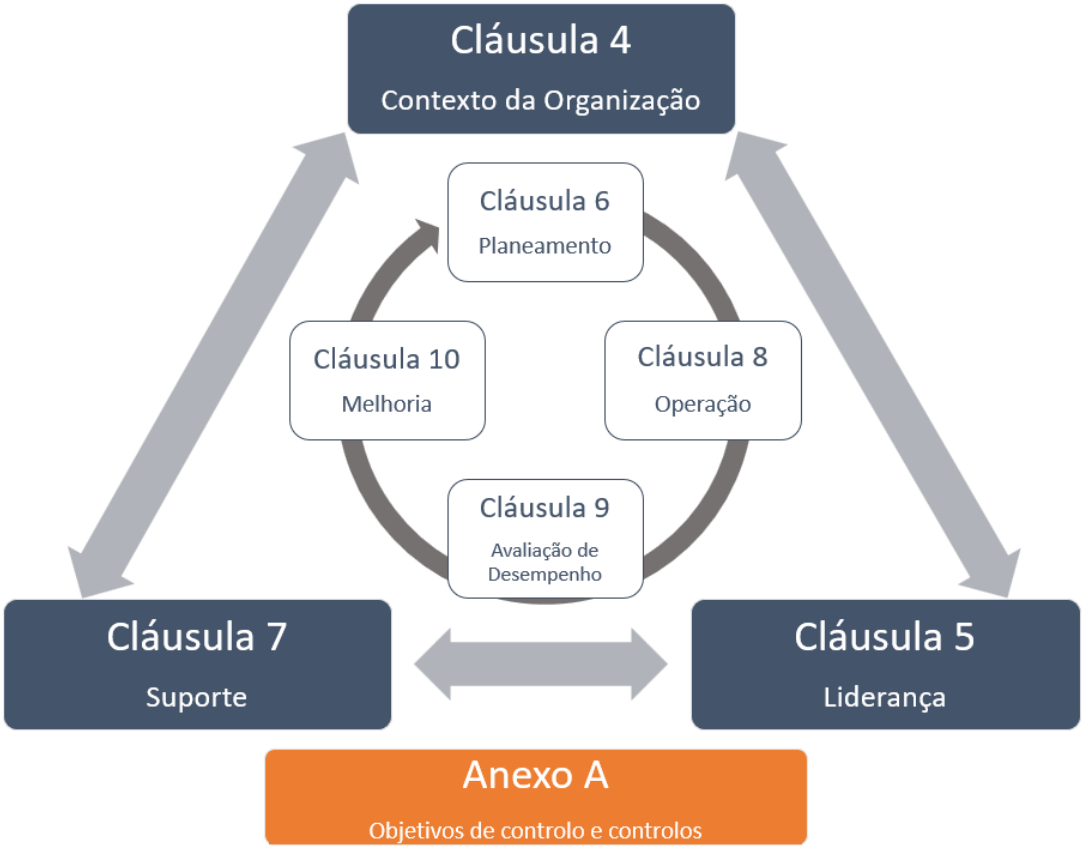


Figura 11: Estrutura global da ISO/IEC 27001 fonte adaptada de (Integrity, 2023)

Como foi referido anteriormente, o Anexo A da ISO/IEC 27001 define e específica os objetivos de controlo e os controlos de referência definidos em 14 secções, cuja ordem não define o grau de importância. Cada secção tem um número determinado de categorias que por sua vez definem um único objetivo e os controlos a aplicar para atingir o objetivo, a tabela 1 sintetiza as secções, as categorias e objetivos e o número de controlos.

Secção	Controlo de referência (Anexo A)	Num. Categorias	Num. Controlos
A.5	Políticas de segurança da informação	1	2
A.6	Organização de segurança da informação	2	7
A.7	Segurança na gestão de recursos humanos	3	6
A.8	Gestão de ativos	3	10
A.9	Controlo de acesso	4	14
A.10	Criptografia	1	2
A.11	Segurança física e ambiental	2	15
A.12	Segurança de operações	7	14
A.13	Segurança de comunicações	2	7
A.14	Aquisição, desenvolvimento e manutenção de sistemas	3	13
A.15	Relações com fornecedores	2	5
A.16	Gestão de incidentes de segurança da informação	1	7
A.17	Aspetos de segurança da informação na gestão de continuidade do negócio	2	4
A.18	Conformidade	2	8
	14 Secções	**35**	**114**

Tabela 1: Controlos de Referência / Categorias / Controlos ISO/IEC 27001:2013 (Correia, 2016)

A partir da análise documental da norma ISO/IEC 27001 é possível identificar as principais dimensões de segurança que contribuem para a gestão de segurança da informação, como se verifica na figura 12.

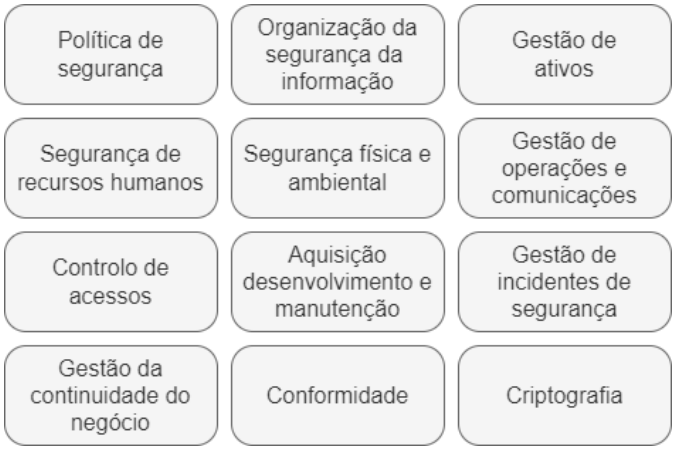


Figura 12: Dimensões de segurança da informação da ISO 27001

Segundo Martins (2021) é importante referir que esta norma pode ser adotada como suporte de um sistema de gestão de privacidade de **dados pessoais** baseado na ISO/IEC 27701 que estende para a privacidade de dados os requisitos e controlos da ISO/IEC 27001.

2.3.4.3 *Objetivos de segurança e de proteção*

A ISO/IEC 27001 garante a confidencialidade, integridade e disponibilidade (CIA), são os principais objetivos de segurança e proteção do padrão. A **confidencialidade** visa garantir que a informação é acessível somente às pessoas autorizadas, implementando mecanismos de criptografia e controlo de acessos. A **integridade** assegura que os dados só podem ser alterados de forma autorizada, protegendo as organizações de ataques de agentes maliciosos, que exploram vulnerabilidades de implementação técnicas para alterar informações. A **disponibilidade** garante que a informação está disponível nos sistemas ou para pessoas autorizadas sempre que for necessária. Para ativos críticos, as organizações necessitam de proteções nos três pilares de segurança (CIA), como na figura 13, a ISO/IEC 27001 assegura essa proteção (Ta-Seen, 2023).

Figura 13: 3 pilares da segurança da informação / objetivos de segurança

2.3.4.4 *Nova versão ISO/IEC 27001:2022*

A versão mais recente, da ISO/IEC 27001:2022, foi lançada em outubro de 2022 e substitui a versão anterior, a ISO/IEC 27001:2013.

SegundoTa-Seen (2023) as principais diferenças entre a versão ISO/IEC 27001:2022 e a ISO/IEC 27001:2013 são:

- Foram realizadas revisões nas cláusulas 4 a 10, especialmente nas cláusulas 4, 6, 8 e 9, com criação de novos conteúdos;
- Identificação das interações dos processos do SGSI necessária para uma visão mais formal e específica do sistema;
- A clausula 6 acrescenta a obrigatoriedade de planeamento e documentação de todas as alterações e a sua disponibilização as partes interessadas (stakeholders);
- As auditorias internas da classe 9 devem avaliar não só os requisitos da ISO/IEC 27001, mas também todos os requisitos organizacionais;
- Os controlos do anexo A foram organizados em 4 domínios ao invés de 14, com 93 controlos ao invés de 114;
- Alguns controlos foram fundidos para reduzir o número de controlos a analisar;

- Foram adicionados 11 novos controlos para colmatar novas tendências e novas tecnologias, como segurança na nuvem, prevenção de fuga de dados, filtragem na web, entre outros;

Em resumo, a ISO/IEC 27001:2022 é uma atualização significativa da norma anterior, que fornece uma abordagem mais ampla e abrangente para a proteção da informação, dando maior ênfase à governança, proteção de dados pessoais e gestão de riscos.

A Figura 14 apresenta o resumo das alterações mais significativas da ISO/IEC27001:2022 e uma comparação com a ISO/IEC27001:2013 baseada na publicação de Kosutic (2023).

Figura 14: Resumo alterações ISO/IEC 27001:2022 baseado em (Kosutic, 2023).

2.3.5 *ISO/IEC 27002*

ISO/IEC 27002 *"Information security, cybersecurity and privacy protection - Information security controls"*.

Standard internacional, usado como referência para a implementação do SGSI baseado na ISO/IEC 27001, fornece um guia de boas práticas com um vasto conjunto de controlos de segurança tendo uma abrangência mais ampla que a ISO/IEC 27001 (*ISO/IEC 27002* 2022).

Segundo Calder (2009) A ISO/IEC 27002 é um guia de boas práticas para segurança das tecnologias de informação. Publicado em julho de 2005, substituiu a ISO/IEC 17799:2000.

A partir de 2008, este padrão foi renumerado (sem quaisquer alterações) para ISO/IEC 27002:2005. Pode servir como uma guia de boas práticas para desenvolver padrões e práticas efetivas de gestão da segurança da informação e ajudar a construir confiança em atividades entre organizações. A ISO/IEC 27002 é quase três vezes maior do que o ISO/IEC 27001, com 126 páginas, das quais 11 são matérias introdutórias e 96 páginas detalham os controlos de segurança da informação. Este padrão tem 16 cláusulas, conforme mostrado abaixo:

1. Introdução;
2. Âmbito;
3. Termos e definições;
4. Estrutura do padrão;
5. Avaliação e tratamento de riscos;
6. Política de segurança;
7. Organização de segurança de informação;
8. Gestão de ativos;
9. Segurança de recursos humanos;
10. Segurança física e ambiental;
11. Gestão de comunicações e operações;
12. Controlo de acessos;
13. Aquisição, desenvolvimento e manutenção de sistemas de informação;
14. Gestão de incidentes de segurança da informação;
15. Gestão da continuidade de negócio;
16. Conformidade;

As onze cláusulas numeradas de cinco a quinze contêm os controlos especificados no Anexo A da ISO/IEC 27001 e essas cláusulas contêm 39 categorias de segurança. A numeração dos controlos é a mesma em ambas as normas.

ISO/IEC 27002:2022

No que diz respeito à transição da ISO/IEC 27002:2013 para a ISO/IEC 27002:2022, é importante destacar que esta atualização tem como objetivo manter a relevância da norma e alinhá-la com as mudanças no panorama da segurança da informação. A ISO/IEC 27002:2022 traz novos controlos e atualizações para abordar desafios emergentes, fornecer orientações mais abrangentes e garantir a adoção de práticas atualizadas.

Com esta nova versão, a ISO/IEC 27002 pretende responder às exigências do ambiente digital em constante evolução, abordando temas como segurança na nuvem, segurança móvel, segurança na Internet das Coisas (IoT) e proteção de dados pessoais.

É relevante salientar que a norma ISO/IEC 27002:2022 disponibiliza em anexos tabelas de correspondência entre a ISO/IEC 27002:2013 e a ISO/IEC 27002:2022, nos dois sentidos. Isso é bastante útil para as organizações que pretendem realizar a transição para a nova versão da ISO/IEC 27001:2022, uma vez que podem encontrar todos os controlos devidamente mapeados. A Figura 15 apresenta um excerto da Tabela B.2 com os mapeamentos.

ISO/IEC 27002:2013 control identifier	ISO/ IEC 27002:2022 control identifier	Control name according to ISO/IEC 27002:2013
5		Information security policies
5.1		Management direction for information security
5.1.1	5.1	Policies for information security
5.1.2	5.1	Review of the policies for information security
6		Organization of information security

Figura 15: Correlação ISO/IEC 27002:2013 e ISO/IEC 27002:2022 (*ISO/IEC 27002* 2022)

2.3.6 *ISO/IEC 27003*

ISO/IEC 27003 *"Information technology - Security techniques - Information security management systems - Guidance"*.

A ISO 27003 é um padrão internacional que fornece orientações para a implementação e gestão de um Sistema de Gestão de Segurança da Informação (SGSI), conforme com a norma ISO 27001, atualmente encontra-se na versão 2017.

O objetivo da ISO 27003 é fornecer um conjunto abrangente de diretrizes e recomendações para ajudar as organizações a estabelecer, implementar, manter e melhorar continuamente um SGSI. O padrão é destinado a todas as organizações, independentemente do seu tamanho, tipo ou setor, que desejam proteger a confidencialidade, integridade e disponibilidade dos seus ativos de informação. Algumas dessas diretrizes incluem:

- Desenvolver uma política de segurança da informação
  Estabelecer uma política abrangente que cubra todos os aspetos da segurança da informação, incluindo responsabilidades, requisitos de conformidade, objetivos de segurança e gestão de riscos.
- Definição do âmbito do SGSI
  Identificar e documentar que informações, sistemas e processos devem ser abrangidos no SGSI.
- Avaliação de riscos
  Identificar e avaliar os riscos de segurança da informação, para poderem ser implementadas medidas de segurança adequadas tendo em conta a mitigação dos riscos.
- Implementar controlos de segurança
  Escolher e implementar os controlos de segurança necessários para proteger as informações e sistemas identificados no âmbito do SGSI.
- Monitorização e revisão
  Criar um processo contínuo de monitorização, análise e revisão do SGSI, para garantir que as medidas de segurança permanecem eficazes e relevantes ao longo do tempo.
- Melhoria contínua
  Identificar oportunidades de melhoria contínua para o SGSI, através da realização de auditorias internas, revisão pela gestão e outros mecanismos.
- Integração com outros processos de negócio
  Garantir que o SGSI esteja alinhado com outros processos de negócio e que haja

comunicação adequada entre as partes interessadas, para garantir que os requisitos de segurança sejam cumpridos em toda a organização.

É relevante enfatizar que a ISO/IEC 27003 não tem caráter certificativo, mas sim orientativo para a implementação de SGSI. Para obter a certificação de um SGSI, a organização deve seguir aos requisitos da norma ISO 27001 e passar por uma auditoria externa realizada por uma entidade de certificação acreditada (*ISO/IEC 27003* 2017).

2.3.7 *ISO/IEC 27005*

ISO/IEC 27005 *"Information security, cybersecurity and privacy protection - Guidance on managing information security risks"*.

A ISO/IEC 27005 identifica as necessidades das organizações no que diz respeito aos **riscos** de segurança da informação e alinha com os conceitos da ISO/IEC 27001 e com os controlos da ISO/IEC 27002.

Fornece uma framework e orientações para identificar, avaliar, tratar e monitorizar os riscos de segurança da informação numa organização. O seu objetivo principal é ajudar as organizações a estabelecerem um processo estruturado e eficaz para a gestão de riscos, com o intuito de proteger os ativos de informação e garantir a continuidade dos negócios.

Algumas das suas principais características representadas graficamente na Figura 16 incluem (Bastos, 2022; *ISO/IEC 27005* 2022):

1. Contexto Organizacional
   Orienta as organizações a compreenderem o contexto em que operam, considerando objetivos organizacionais, âmbitos, responsabilidades, requisitos legais, regulamentares e contratuais, bem como as expectativas das partes interessadas.
2. Processo de Gestão de Riscos
   Estabelece diretrizes para a implementação de um processo de gestão de riscos de segurança da informação, abrangendo etapas como identificação, análise, avaliação, tratamento e monitorização de riscos.
3. Identificação de Ativos de Informação
   Enfatiza a importância da identificação dos ativos de informação relevantes para

a organização, como dados, sistemas, infraestrutura e recursos relacionados com segurança da informação.

4. Avaliação de Riscos
   Fornece orientações para a avaliação de riscos, incluindo a identificação de ameaças, vulnerabilidades e potencias impactos, bem como a determinação do nível de risco associado a cada ativo de informação.

5. Tratamento de Riscos
   Aborda opções de tratamento de riscos, como a implementação de controlos de segurança apropriados, mitigação de riscos por meio de medidas de proteção e a definição de planos de ação para trabalhar com os riscos identificados.

6. Monitorização e Revisão
   Destaca a importância da monitorização contínua dos riscos de segurança da informação e da revisão regular do processo de gestão de riscos, a fim de garantir a eficácia dos controlos implementados e a identificação de novos riscos emergentes.

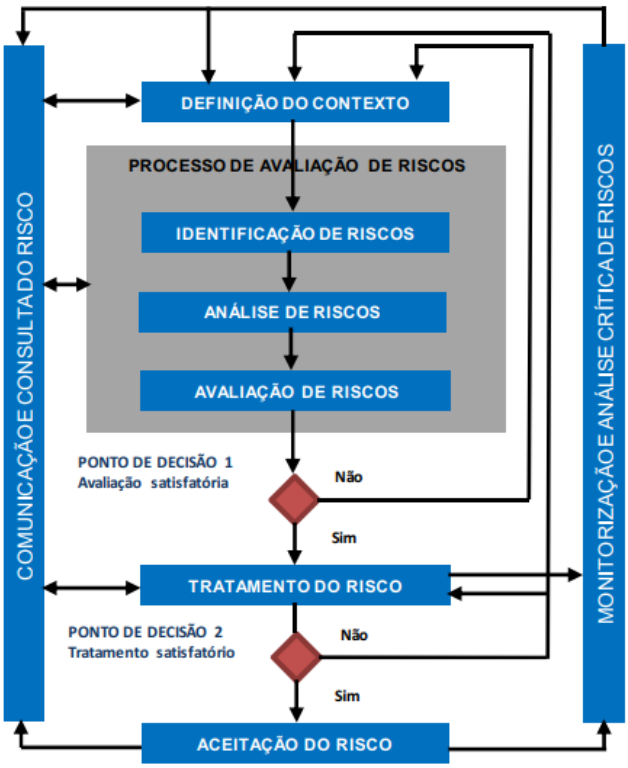


Figura 16: Processo iterativo de Gestão de Risco ISO 27005 (*ISO/IEC 27005* 2022)

2.3.8 *Outras Normas da família 27000*

A família de normas ISO/IEC 27000 é uma série de normas internacionais da segurança da informação. Essas normas fornecem diretrizes e recomendações para implementar uma abordagem de gestão da segurança da informação, incluindo a identificação, análise e gestão de riscos, seleção e implementação de medidas de segurança, monitorização e revisão do sistema de gestão da segurança da informação, fornecendo uma abordagem abrangente para garantir a confidencialidade, integridade e disponibilidade das informações garantindo a conformidade com os requisitos legais e regulatórios.

É amplamente aceite e utilizada em todo o mundo como um padrão para a implementação de um SGSI e é também usada como ponto de referência para atender às exigências legais e regulatórias relacionadas com segurança da informação.

Esta família é composta por várias normas, cada uma com um objetivo específico. Atualmente, existem mais de 20 normas na família ISO/IEC 27000. Algumas das principais normas incluem:

- ISO/IEC 27001
  Norma específica para a implementação e manutenção de um SGSI e fornece diretrizes para a implementação de controles de segurança da informação.
- ISO/IEC 27002
  Fornece diretrizes para a implementação de controlos técnicos e referenciais para garantir a segurança da informação.
- ISO IEC 27003
  Fornece diretrizes para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI)
- ISO/IEC 27005
  Fornece diretrizes para gestão de riscos.
- ISO/IEC 27006
  Fornece diretrizes para a certificação de um SGSI.
- ISO/IEC 27018
  Fornece diretrizes para proteção de dados pessoais.

Além dessas, existem outras normas na família ISO/IEC 27000 que tratam de temas específicos, como segurança de dados em ambientes de nuvem, gestão de incidentes de segurança, garantia e continuidade de negócios, entre outros. A figura 17 ilustra a conexão entre as normas da série ISO/IEC 27000.

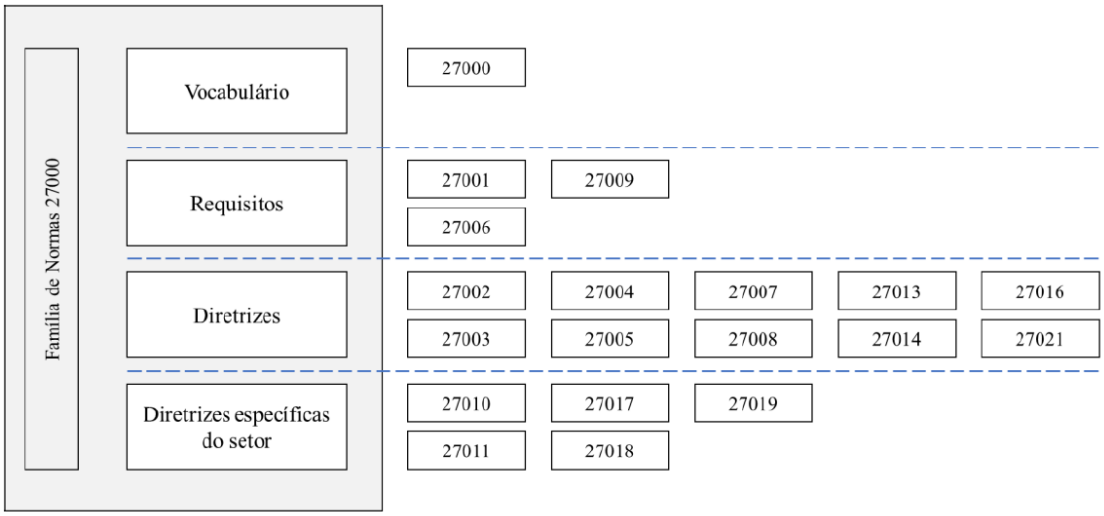


Figura 17: Relação entre as famílias da ISO/IEC 27000 adaptado de (*ISO/IEC 27000* 2018)

2.3.8.1 *ISO/IEC 27000*

ISO/IEC 27000 *"Information technology - Security techniques - Information security management systems - Overview and vocabulary"*.

A norma ISO/IEC 27000, é a norma inicial da família de normas ISO/IEC 27000 e fornece uma visão geral dos conceitos, termos e definições relacionados com segurança da informação. Atualmente encontra-se na versão 2018 (*ISO/IEC 27000* 2018).

A ISO/IEC 27000 não estabelece requisitos específicos para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI), mas fornece orientações gerais e um vocabulário comum que é aplicável a todas as organizações. É destinada a ajudar as organizações a perceber os princípios da segurança da informação e a estabelecer uma base sólida para o desenvolvimento de políticas, processos e controlos de segurança.

Destaca ainda a importância da liderança e do comprometimento da gestão de topo no estabelecimento de uma cultura de segurança da informação nas organizações.

Abaixo é apresentada a tabela 2 com algum dos termos mais regulares definidos na ISO/IEC 27000.

Secção	Termo	Definição
3.1	**Controlo de acesso**	meios para assegurar que o acesso aos bens é autorizado e limitado com base em requisitos de negócios e de segurança.
3.2	**Ataque**	tentativa de destruir, expor, alterar, inutilizar, roubar ou obter acesso não autorizado, ou a utilização não autorizada de um ativo.
3.3	**Auditoria**	processo sistemático, independente e documentado para a obtenção de evidência de auditoria e avaliá-la objetivamente para determinar a extensão do cumprimento dos critérios de auditoria.
3.5	**Autenticação**	prestação de garantia de que uma característica reivindicada por uma entidade é correta.
3.6	**Autenticidade**	propriedade que comprova que uma entidade é o que diz ser.
3.7	**Disponibilidade**	propriedade de ser acessível e utilizável por uma entidade autorizada.
3.10	**Confidencialidade**	propriedade que a informação não é disponibilizada ou divulgada a pessoas não autorizadas, entidades ou processos.
3.14	**Controlo**	meio de gestão de risco.
3.36	**Integridade**	propriedade de plenitude de exatidão.
3.52	**Políticas**	intenções e estratégia de uma organização, expressas pela administração.
3.54	**Processo**	conjunto de atividades inter-relacionadas que transforma entradas (inputs) em saídas (outputs).

Contínua na próxima página...

Secção	Termo	Definição
3.55	**Confiabilidade**	propriedade de comportamento e resultados consistentes.
3.56	**Requisito**	expectativa ou necessidade expressa, geralmente implícita ou obrigatória.
3.74	**Ameaça**	causa potencial de um incidente indesejado, que pode resultar em danos para um sistema ou organização.
3.77	**Vulnerabilidade**	fraqueza de um ativo ou controlo que pode ser explorado por uma ou mais ameaças.

Tabela 2: Termos e definições da ISO/IEC 27000 (*ISO/IEC 27000* 2018)

2.3.8.2 *Norma ISO/IEC 27701*

ISO/IEC 27701 *"Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines"*.

A norma ISO/IEC 27701 é uma extensão da norma ISO/IEC 27001, que se concentra na privacidade da informação, estabelece os requisitos e fornece orientações para um Sistema de Gestão de Privacidade da Informação, permitindo que as organizações protejam e gerenciem de forma eficaz os dados pessoais.

Fornece um conjunto abrangente de controlos e práticas que ajudam as organizações a atender às exigências de privacidade de dados e cumprir as regulamentações relevantes, como o Regulamento Geral de Proteção de Dados (RGPD) e aborda aspetos como a recolha, o processamento, o armazenamento e a divulgação de informações pessoais, além de envolver a gestão de riscos e a conformidade com as políticas de privacidade.

A norma ISO/IEC 27701 também oferece diretrizes sobre como as organizações podem estabelecer e manter um programa de privacidade da informação, incluindo a definição de responsabilidades, a realização de avaliações de impacto de privacidade, o estabelecimento de medidas de segurança adequadas e a condução de auditorias internas.

A implementação da ISO/IEC 27701 permite que as organizações demonstrem compromisso com a privacidade da informação e contribui para, a confiança dos clientes e

partes interessadas, minimização de riscos relacionados com violação de dados pessoais e ajuda as organizações a cumprir obrigações legais e éticas no tratamento de informações pessoais.

Em resumo, a norma é fundamental para organizações que processam informações pessoais, como dados de clientes, funcionários e parceiros comerciais, e precisam de garantir a proteção dessas informações, bem como para cumprir com as leis e regulamentações de privacidade aplicáveis (*ISO/IEC 27701* 2019).

2.4 OUTROS STANDARDS E METODOLOGIAS

Nesta secção, serão abordados outros standards e metodologias frequentemente utilizados no desenvolvimento de sistemas de segurança da informação, tais como o IEC-62443, COBIT, ITIL e NIST. Estes padrões oferecem orientações relevantes para reforçar a segurança dos ativos de informação. A incorporação destas referências pode enriquecer a abordagem de segurança adotada pelas organizações.

2.4.1 *IEC 62443*

A norma IEC 62443, também conhecida como ISA/IEC 62443, é uma norma internacional que estabelece diretrizes e requisitos para a segurança cibernética de sistemas de automação e controlo industrial. Foi desenvolvida pela International Society of Automation (ISA) e pela International Electrotechnical Commission (IEC) com o objetivo de fornecer orientações claras e práticas para proteger os sistemas industriais contra ameaças cibernéticas.

O IEC 62443 aborda os desafios específicos de segurança enfrentados pelos sistemas de controlo industrial, utilizados em setores como energia, transformação, petróleo e gás, transporte e infraestruturas críticas. Esses sistemas são fundamentais para a operação segura e confiável de instalações industriais que podem ser alvos de ataques cibernéticos maliciosos que visam interromper processos, causar danos ou obter acesso não autorizado a informações sensíveis.

A norma IEC 62443 é uma série de standards que abrange diversos aspetos da segurança cibernética em sistemas de automação e controlo industrial (ICS) é composta por várias partes, cada uma delas aborda aspetos específicos da segurança cibernética, fornecendo um conjunto abrangente de diretrizes e requisitos para a implementação de medidas de segurança nesses sistemas e abrangendo diferentes aspetos da segurança, desde a gestão de riscos até a implementação de controlos de segurança específicos.

Alguns dos principais tópicos abordados incluem:

1. Avaliação de riscos e definição de níveis de segurança
   A norma fornece orientações sobre como realizar uma avaliação de riscos adequada, identificando as ameaças e vulnerabilidades específicas dos sistemas de controlo industrial. Com base nessa avaliação, são definidos os níveis de segurança necessários para proteger os ativos críticos.

2. Controlos de segurança
   A IEC 62443 apresenta uma série de controlos de segurança que devem ser implementados para proteger os sistemas de automação e controlo. Esses controlos incluem medidas técnicas, como autenticação, criptografia, controlo de acesso e deteção de intrusões, bem como controlos organizacionais, como políticas de segurança e consciencialização dos recursos humanos.

3. Gestão de alterações
   A norma aborda a importância de um processo estruturado para gerir alterações nos sistemas de controlo industrial, garantindo que as alterações sejam efetuadas de forma controlada e segura, minimizando os riscos de falhas de segurança.

4. Monitorização e resposta a incidentes
   A IEC 62443 destaca a necessidade de estabelecer sistemas de monitorização contínua e prontidão para responder a incidentes de segurança cibernética. Envolvendo a deteção rápida de atividades suspeitas, a investigação de incidentes e a implementação de medidas corretivas apropriadas.

A adoção do standard IEC 62443 trás benefícios significativos para as organizações que dependem de sistemas de automação e controlo industrial, ajuda a reduzir os riscos de interrupções operacionais, protege os ativos críticos, melhora a resiliência do sistema e aumenta a confiança dos stakeholders (*ISA/IEC 62443* 2020).

2.4.2 *COBIT*

COBIT, abreviação de "Control Objectives for Information and Related Technologies"é uma estrutura de governança e gestão de TI reconhecida internacionalmente. Desenvolvido pelo ISACA (Information Systems Audit and Control Association), o COBIT oferece orientações e práticas recomendadas para auxiliar as organizações a alcançarem objetivos de negócio por meio do uso efetivo e seguro da tecnologia da informação.

O COBIT foi desenvolvido para auxiliar as organizações a estabelecerem um sistema abrangente de governança de TI, abordando questões relacionadas com a gestão de riscos, o controlo interno, a entrega de valor e a conformidade regulatória. Esta framework fornece uma estrutura de processos, objetivos de controlo, indicadores de desempenho e as melhores práticas que podem ser aplicadas em diversas áreas e setores.

Princípios COBIT

Os princípios do COBIT fornecem uma base sólida para a sua aplicação. Enfatizam a importância de satisfazer as necessidades das partes interessadas, abranger todos os aspetos da empresa, adotar uma abordagem integrada, uma visão holística e separar claramente as atividades de governança das atividades de gestão.

Os princípios apresentados a seguir são fundamentais para o COBIT e orientam a sua aplicação para alcançar uma governança e gestão eficaz de TI a figura 18 apresenta esses princípios:

1. **Atender às necessidades das partes interessadas**
   Destaca a importância de identificar, compreender e atender às necessidades das partes interessadas relevantes, como acionistas, clientes, colaboradores e reguladores. Assegura que as decisões e ações relacionadas com governança e gestão de TI sejam orientadas para alcançar resultados alinhados com os objetivos estratégicos da organização.
2. **Cobrir a empresa de ponta a ponta**
   Abrange todas as áreas e processos relacionados com governança e gestão de TI numa organização, desde a definição de estratégias e políticas até a implementação

e monitorização dos controlos. Proporcionando uma visão global e abrangente da governança de TI, garantindo que todas as partes relevantes sejam consideradas e que nenhum aspeto crítico seja negligenciado.

3. **Aplicar um framework único e integrado**
   Promove uma abordagem integrada, na qual todos os componentes de governança e gestão de TI são inter-relacionados e trabalham em conjunto para alcançar os objetivos organizacionais. incluindo processos, estruturas organizacionais, políticas, padrões e ferramentas.

4. **Permitir uma abordagem holística**
   Incentiva uma visão holística da governança e gestão de TI, considerando os diferentes aspetos, como pessoas, processos, tecnologia e informação, reconhece a interdependência entre esses elementos e a importância em os abordar de forma integrada.

5. **Distinguir a governança da gestão**
   Distingue claramente as responsabilidades e atividades de governança das responsabilidades e atividades de gestão. Define os papéis e responsabilidades dos diferentes níveis da organização, garantindo uma separação clara de funções e uma governança eficaz.

Figura 18: Princípios COBIT (itsmnapratica, 2023)

Características

A seguir enumeram-se algumas das principais características do COBIT:

1. Orientação abrangente
   Abrange todas as áreas de governança e gestão de TI, incluindo estratégia, entrega de serviços, gestão de riscos e conformidade.
2. Baseado em processos
   Adota uma abordagem baseada em processos, fornecendo uma estrutura para a definição, implementação, monitorização e melhoria contínua dos processos de TI.
3. Alinhamento com objetivos de negócio
   Ajuda as organizações a alinhar os objetivos de TI com os objetivos de negócio, garantindo que a TI esteja direcionada para agregar valor e suportar as metas definidas pela organização.
4. Ênfase na governança
   Enfatiza a importância da governança de TI, fornecendo orientações para a definição de estruturas de governança, papéis e responsabilidades, e a criação de mecanismos de monitorização e controlo.
5. Adaptabilidade
   O COBIT é flexível e pode ser adaptado às necessidades específicas de cada organização, permitindo que ela selecione e implemente os processos e controlos relevantes para seu contexto.

Benefícios

Ao adotar o COBIT, as organizações podem estabelecer uma estrutura sólida para a governança e gestão de TI, melhorando a eficiência, a transparência, a responsabilidade e a tomada de decisões relacionadas com TI. O COBIT ajuda a garantir a utilização efetiva dos recursos de TI, a minimização de riscos e a entrega de valor aos stakeholders, contribuindo para o sucesso e a sustentabilidade dos negócios:

1. Melhoria da governança e gestão de TI
   Ajuda as organizações a estabelecer práticas sólidas de governança e gestão de TI, promovendo a transparência, responsabilidade e eficácia dos processos de TI.
2. Alinhamento estratégico
   Auxilia na integração dos objetivos de TI com os objetivos de negócio, garantindo que a TI esteja alinhada com as necessidades e direções estratégicas da organização.
3. Controlo e gestão de riscos
   Fornece orientações para estabelecer controlos internos efetivos e gestão de riscos relacionados com TI, auxiliando na proteção de ativos e na prevenção de incidentes e violações de segurança.
4. Melhoria contínua
   Apoia a procura contínua pela excelência em governança e gestão de TI, fornecendo um ciclo de melhoria contínua baseado na análise, definição, implementação e monitorização dos processos de TI.

(ISACA, 2023)

2.4.3 *ITIL*

ITIL (Information Technology Infrastructure Library) é uma framework de boas práticas para a gestão de serviços de TI em que os vários processos comunicam uns com os outros. Cada um tem o seu próprio papel por forma a que, no final, possam dar resposta a duas questões: melhoria contínua e a satisfação do cliente (Santos, 2016). Desenvolvida pelo governo britânico na década de 1980, o ITIL tornou-se uma referência global para a melhoria dos processos de entrega de serviços de TI.

O ITIL é uma abordagem amplamente adotada para a gestão de serviços de tecnologia da informação. Fornece um conjunto de melhores práticas e orientações para ajudar as organizações a fornecerem serviços de TI de alta qualidade e alinhados com as necessidades do negócio.

O ITIL abrange uma variedade de áreas-chave da gestão de serviços de TI, incluindo a estratégia de serviço, o desenho do serviço, a transição do serviço, a operação do serviço

e a melhoria contínua do serviço. Cada uma dessas áreas é detalhada em processos e práticas que visam melhorar a eficiência, a qualidade e a entrega dos serviços de TI, estas áreas são demonstradas na figura19:

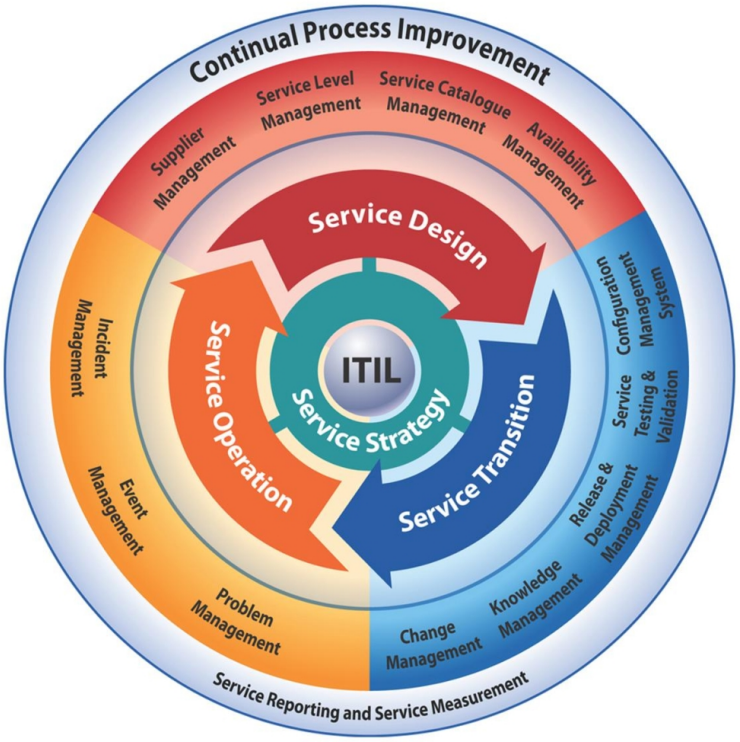


Figura 19: Ciclo de Vida de um Serviço - ITIL (despnet, 2023)

1. Estratégia do Serviço
   Nesta fase, são definidos os objetivos estratégicos de TI alinhados com os objetivos de negócio da organização, identificados os serviços necessários e definida a estratégia para a sua entrega.

2. Desenho do Serviço
   Aqui são desenvolvidos os planos e especificações para a implementação dos serviços de TI, definidos os requisitos, a arquitetura, os processos e as políticas necessárias para a entrega dos serviços.

3. Transição do Serviço
   Nesta fase, os serviços são construídos, testados e implementados. São realiza-

das as atividades de gestão de alterações, gestão de configurações e gestão de implementações, garantindo uma transição fluida dos serviços para a produção.

4. Operação do Serviço
   Fase em que os serviços de TI são executados e entregues aos utilizadores finais, são realizadas atividades como gestão de incidentes, gestão de problemas, gestão de pedidos e gestão de acesso, garantindo a disponibilidade e o desempenho dos serviços.

5. Melhoria Contínua do Serviço
   Esta fase abrange a análise e melhoria contínua dos serviços de TI. São realizadas avaliações de desempenho, identificadas oportunidades de melhoria e implementadas ações corretivas para aperfeiçoar a qualidade e eficiência dos serviços.

Caracteristicas

Algumas das principais características do ITIL incluem:

1. Orientação para processos
   Promove uma abordagem baseada em processos para a gestão de serviços de TI, garantindo uma estrutura clara e consistente para a execução das atividades.

2. Ênfase no valor do serviço
   Enfatiza a importância de fornecer valor aos utilizadores finais através da entrega de serviços de TI que atendam às suas necessidades e expetativas.

3. Abordagem holística
   Considera todos os aspetos envolvidos na gestão de serviços de TI, incluindo pessoas, processos, tecnologia e parcerias, promovendo uma visão abrangente e integrada.

4. Adoção flexível
   O ITIL é flexível e adaptável, permitindo que as organizações implementem apenas as partes relevantes conforme as suas necessidades e recursos.

5. Melhoria contínua
   Incentiva a melhoria contínua dos serviços de TI através da análise de desempenho, feedback dos utilizadores e implementação de ações corretivas.

Os benefícios da adoção do ITIL incluem:

1. Melhoria da qualidade dos serviços
   Fornece diretrizes e melhores práticas que ajudam a melhorar a qualidade e a consistência dos serviços de TI.
2. Alinhamento com as necessidades do negócio
   Promove uma abordagem orientada para o valor, garantindo que os serviços de TI estejam alinhados com as necessidades e objetivos do negócio.
3. Maior eficiência e produtividade
   Ajuda a otimizar os processos de entrega de serviços, reduzindo custos e aumentando a eficiência e a produtividade da organização.
4. Gestão de riscos melhorada
   Inclui práticas para a gestão de riscos de TI, ajudando a identificar e mitigar potenciais ameaças e vulnerabilidades.
5. Maior satisfação do utilizador
   Ao fornecer serviços de TI de qualidade e alinhados com as necessidades dos utilizadores, o ITIL contribui para a satisfação e a confiança dos utilizadores finais.

(Axelos, 2023)

2.4.4 *NIST*

O National Institute of Standards and Technology (NIST) é uma entidade não reguladora que promove a inovação através do avanço da ciência, definição de padrões e tecnologia de medição. O NIST Cybersecurity Framework (NIST CSF) é composto por normas, diretrizes e práticas recomendadas que auxiliam as organizações a aperfeiçoar a gestão dos riscos de segurança cibernética.

O NIST CSF foi concebido para ser suficientemente flexível para se adaptar aos processos de segurança já existentes em qualquer organização e em qualquer setor. Oferece um ponto de partida sólido para implementar segurança da informação e gestão de riscos de segurança cibernética em praticamente qualquer organização do setor privado nos Estados Unidos.

Em 12 de fevereiro de 2013, foi emitida a Ordem Executiva (EO) 13636: "Melhorando a Segurança Cibernética da Infraestrutura Crítica". Esta ordem marcou o início do trabalho do NIST com o setor privado dos Estados Unidos para "identificar padrões de consenso voluntários existentes e melhores práticas da indústria, a fim de os incorporar numa Estrutura de Segurança Cibernética"[2]. O resultado dessa colaboração foi a versão 1.0 do NIST Cybersecurity Framework.

O Cybersecurity Enhancement Act (CEA) de 2014 ampliou os esforços do NIST no desenvolvimento do Cybersecurity Framework. Atualmente, o NIST CSF continua a ser uma das framewaorks de segurança mais adotada em todos os setores dos Estados Unidos.

Estrutura central do NIST Cybersecurity Framework

A Framework de Cibersegurança do NIST inclui elementos como funções, categorias, subcategorias e referências informativas.

As funções fornecem uma visão geral dos princípios de segurança cibernética e melhores práticas. Não devem ser encaradas como etapas sequenciais, mas sim como atividades que devem ser executadas de forma simultânea e contínua para criar uma cultura operacional que aborde os riscos dinâmicos da segurança cibernética.

As categorias e subcategorias oferecem planos de ação mais concretos para departamentos ou processos específicos numa organização, ajudando a direcionar as medidas de segurança apropriadas.

As principais funções da NIST demonstradas na figura 20 incluem:

- **Identificar**
  Desenvolver uma compreensão clara dos ativos de informação, sistemas, ameaças e vulnerabilidades relacionadas com a segurança cibernética.
- **Proteger**
  Implementar medidas de segurança para garantir a proteção adequada dos ativos de informação e sistemas contra ameaças cibernéticas.

2 "Identify existing voluntary consensus standards and industry best practices to incorporate into a Cybersecurity Framework" (EO 13636)

- **Detetar**
  Estabelecer mecanismos de deteção para identificar de forma imediata atividades cibernéticas maliciosas ou não autorizadas.
- **Responder**
  Desenvolver e implementar planos de resposta para tratar de forma eficaz incidentes de segurança cibernética.
- **Recuperar**
  Restaurar as capacidades operacionais e os serviços de informação afetados por incidentes de segurança cibernética e realizar melhorias contínuas para prevenir futuros incidentes.

Figura 20: Principais funções da NIST (NIST, 2023)

Estas funções e categorias do NIST fornecem uma estrutura sólida para ajudar as organizações a fortalecer a sua postura de segurança cibernética e mitigar os riscos associados às ameaças cibernéticas.

O NIST CF não especifica os detalhes de como realizar o inventário de dispositivos e sistemas físicos, nem fornece um método específico para inventariar plataformas de

software e aplicativos. Em vez disso, apresenta uma lista de tarefas a serem concluídas. A organização tem a liberdade de escolher o seu próprio método para realizar o inventário, conforme as suas necessidades e requisitos específicos.

Caso uma organização necessite de orientações adicionais, é possível consultar as referências informativas aos controlos relacionados de outras normas complementares. Essas referências podem fornecer diretrizes mais detalhadas sobre os processos de inventário.

O NIST CSF oferece flexibilidade nesse aspeto, permitindo que as organizações escolham as ferramentas e abordagens que melhor atendam às suas necessidades de gestão de riscos de segurança cibernética. Dessa forma, as organizações podem adaptar o processo de inventário conforme as suas capacidades, recursos e ambientes operacionais.

Benefícios da adoção do NIST CF

A adoção do NIST CF pode trazer uma série de benefícios para as organizações. Abaixo estão alguns dos principais benefícios:

1. Melhoria da postura de segurança cibernética
   Fornece uma estrutura abrangente para identificar, avaliar e gerir riscos de segurança cibernética.
2. Alinhamento com padrões e regulamentações
   Foi desenvolvida tendo em consideração vários padrões, regulamentações e frameworks existentes.
3. Abordagem flexível e adaptável
   Projetado para ser flexível e adaptável a diferentes organizações, setores e tamanhos.
4. Melhoria da comunicação e colaboração
   Fornece uma linguagem comum e estrutura para comunicação sobre segurança cibernética entre as partes interessadas.
5. Foco em resultados de negócios
   Ajuda as organizações a conectar a segurança cibernética aos objetivos de negócios.
6. Melhoria contínua
   Promove uma abordagem de melhoria contínua da segurança cibernética.

No geral, a adoção do NIST CF pode ajudar as organizações a fortalecerem a sua segurança cibernética, mitigar riscos e a proteger os seus ativos de informação, resultando numa maior confiança das partes interessadas e resiliência contra ameaças cibernéticas (IBM, 2023).

2.4.5 *Comparação de metodologias*

Cada uma das frameworks e padrões apresentados anteriormente possuem as suas próprias especificidades e áreas de aplicação. A escolha de qual utilizar ou combinar depende das necessidades e objetivos específicos de cada organização relativamente à governança, gestão de TI, segurança da informação e entrega de serviços de TI.

A tabela 3 apresenta uma comparação entre os frameworks e padrões ITIL, COBIT, NIST e ISO/IEC 27001, destacando as principais características de cada um deles:

Norma	**Principal Foco**	**Objetivos**	**Dominios de Aplicação**	**Benefícios**
ITIL	Gestão de Serviços de TI	Melhorar a entrega de serviços de TI, alinhando-os com as necessidades do negócio	Gestão de serviços de TI	Aumento da eficiência e eficácia dos serviços de TI, melhor alinhamento com as necessidades do negócio, maior satisfação dos utilizadores
COBIT	Governança e Gestão de TI	Garantir o alinhamento entre TI e os objetivos de negócio, fornecer controlos e diretrizes para a gestão de TI	Governança de TI, Gestão de Riscos e Controlo, Gestão de Programas e Projetos, entre outros	Melhor governança e gestão de TI, maior transparência, conformidade regulatória

NIST	Segurança da Informação	Fornecer diretrizes e padrões de segurança da informação para organizações	Gestão de Riscos, Segurança de Redes, Segurança de Sistemas, Segurança de Dados, entre outros	Fortalecimento da segurança da informação, mitigação de riscos, conformidade regulatória
ISO 27001	Gestão da Segurança da Informação	Estabelecer um sistema de gestão da segurança da informação nas organizações	Políticas de Segurança, Gestão de Riscos, Controlos de Segurança, Monitorização e Melhoria Contínua	Melhor gestão da segurança da informação, conformidade com padrões internacionais, aumento da confiança dos clientes, conformidade regulatória

Tabela 3: Comparação entre ITIL, COBIT, NIST e ISO 27001

2.5 FRAMEWORKS NACIONAIS

As frameworks portuguesas de cibersegurança são conjuntos de diretrizes e boas práticas desenvolvidas especificamente para responder às necessidades e desafios do contexto de cibersegurança em Portugal. Estas frameworks visam fornecer orientações e recomendações às organizações para fortalecer a segurança dos sistemas de informação e proteger dados sensíveis, auxiliando-as no fortalecimento da sua postura de segurança, mitigação de riscos e a enfrentarem os desafios emergentes no campo da cibersegurança.

Em Portugal, existem várias organizações/organismos que trabalham no domínio da cibersegurança:

- **CNCS - Centro Nacional de Cibersegurança**
  O CNCS é uma entidade governamental responsável pela promoção da cibersegurança no país. Este centro disponibiliza várias orientações e recomendações técnicas para as organizações implementarem medidas de segurança adequadas.

- **ENSC - Estratégia Nacional de Segurança do Ciberespaço**
  A ENSC é uma iniciativa que visa definir uma estratégia abrangente para a segurança do ciberespaço em Portugal. Estabelece diretrizes, objetivos e metas para proteção dos sistemas de informação e promoção de uma cultura de cibersegurança no país.
- **RCTS - Rede Ciência, Tecnologia e Sociedade**
  A RCTS é uma rede académica portuguesa que promove a colaboração e partilha de recursos entre instituições de ensino superior e de investigação em Portugal. Embora não seja exclusivamente uma framework de cibersegurança, a RCTS desempenha um papel importante ao fornecer serviços e infraestruturas de rede seguras para as instituições académicas e de investigação.

2.5.1 *Quadro Nacional de Cibersegurança*

O Quadro Nacional de Cibersegurança[3] (QNC) é um documento que estabelece a estratégia nacional de cibersegurança de Portugal, fornecendo uma visão holística do ecossistema de cibersegurança português e as medidas necessárias para proteger as infraestruturas críticas e os sistemas de informação do país contra ciberataques e outras ameaças.

O QNC estabelece as prioridades e objetivos da política nacional de cibersegurança, bem como as medidas necessárias para os alcançar. Fornece orientações para a melhoria da capacidade de resposta e resiliência do país relativamente a ciberataques, bem como a coordenação entre as diferentes partes interessadas no ecossistema cibernético português, incluindo governo, empresas, organizações da sociedade civil e público em geral.

O documento foi elaborado pelo Centro Nacional de Cibersegurança (CNCS), uma entidade portuguesa responsável pela promoção da segurança cibernética em Portugal, em colaboração com várias partes interessadas, incluindo o setor público, privado e académico. O QNC é peça-chave da estratégia nacional de cibersegurança em Portugal, é atualizado periodicamente para responder às novas ameaças e desafios na área da cibersegurança.

3 CNCS | Quadro Nacional de Cibersegurança

2.5.2 *Roteiro para Capacidades Mínimas de Cibersegurança*

O Roteiro para Capacidades Mínimas de Cibersegurança[4] do Centro Nacional de Cibersegurança (CNCS) é um guia que estabelece as capacidades mínimas que as organizações devem ter para garantir a segurança dos seus sistemas de informação. O objetivo do roteiro é ajudar as organizações a identificar e implementar as melhores práticas em cibersegurança, independentemente do tamanho ou setor em que operam.

O roteiro é composto por um conjunto de áreas temáticas de cibersegurança, cada uma com as suas próprias capacidades mínimas recomendadas. As áreas temáticas incluem, por exemplo, gestão de segurança, governança, gestão de riscos, segurança da informação, segurança das redes e sistemas, gestão de incidentes de segurança e continuidade de negócios.

Para cada uma das áreas temáticas, o roteiro estabelece as capacidades mínimas que as organizações devem ter, bem como exemplos de práticas recomendadas para atingir essas capacidades. Além disso, o roteiro também inclui um conjunto de indicadores chave de desempenho (KPIs) que podem ser utilizados para medir o progresso e a eficácia das medidas de segurança implementadas pelas organizações.

O Roteiro para Capacidades Mínimas de Cibersegurança do CNCS é um recurso útil para as organizações que desejam melhorar a segurança dos seus sistemas de informação e garantir a proteção dos seus dados e sistemas. Ao seguir as capacidades mínimas recomendadas, as organizações podem reduzir o risco de sofrerem incidentes de segurança da informação e minimizar os impactos em caso de ocorrência desses incidentes.

2.5.3 *Certificação de maturidade digital «Selos digitais»*

Segundo portugaldigital.gov.pt *possuir um Selo de Maturidade Digital é sinal de confiança, competitividade, progresso e reconhecimento do compromisso com o digital.*

A certificação de maturidade digital é acessível a qualquer organização do setor privado ou público que queira demonstrar que segue as boas práticas no âmbito da transformação digital e cumpre os normativos do Instituto Português da Qualidade (IPQ).

4 CNCS | Roteiro para Capacidades Mínimas de Cibersegurança

As quatro dimensões de certificação são: cibersegurança, acessibilidade, privacidade e sustentabilidade, e cada dimensão tem três níveis de maturidade digital: Bronze, Prata e Ouro.

A certificação é obtida mediante uma auditoria realizada por uma entidade certificadora acreditada pelo Instituto Português de Acreditação (IPAC). Essa certificação oferece benefícios como minimizar a exposição ao cibercrime, aumentar o potencial de interagir com novos clientes, melhorar a capacidade de gerir dados sensíveis, contribuir para o combate às alterações climáticas e incrementar a notoriedade do negócio.

Os selos de certificação de maturidade digital têm reconhecimento mútuo com o Digital with Purpose, promovido pela GeSI - Global Enabling Sustainability Initiative

O CNCS desempenhou um papel ativo no processo de definição dos requisitos técnicos a serem implementados pelos candidatos aos "Selos digitais"e teve um papel importante na elaboração do esquema de certificação correspondente, resultando na publicação da Norma DNP TS 4475-1:2021.

Embora esta certificação não esteja incluída no Quadro Nacional de Certificação da Cibersegurança, o CNCS é responsável por garantir a adequação e atualização dos requisitos técnicos do esquema, em relação aos objetivos de cibersegurança, bem como colaborar com o IPAC nas atividades de acreditação de organismos de certificação.

Para as pequenas e médias empresas que não desejam adotar um sistema de gestão, como o caso da ISO/IEC 27001, por estes serem demasiado onerosos a todos os níveis, os selos de maturidade digital são, de fato, uma excelente ferramenta para demonstrar conformidade digital e consequentemente, transmitir confiança às entidades com as quais se relacionam.

2.6 TRABALHO RELACIONADO

No âmbito do desenvolvimento deste projeto foram efetuadas diversas pesquisas baseadas em palavras-chave por artigos científicos e trabalhos académicos na tentativa de encontrar o estado de arte relativamente à implementação de um SGSI em organizações que tenham em consideração a conformidade com as normas da família ISO/IEC 27000,

não esquecendo a componente de controlos industrias.

Como resultado destacaram-se quatro dissertações de mestrados que implementam as temáticas de implementação de SGSI e sistemas de controlo industriais ICS três de âmbito nacional e uma internacional.

Dos muitos documentos lidos e alisados, estes foram os selecionados por oferecerem uma visão mais ampla do tema e problemática a desenvolver neste documento:

- Oliveira em 2015 realiza na Universidade Lusíada uma dissertação de mestrado intitulada de «Contribuição para a estruturação do sistema integrado de gestão do grupo Cooprofar - Medlogcom integração da gestão de segurança da informação» (Oliveira, 2015).
- Em 2016 Correia realiza uma tese de mestrado na Universidade Nova de Lisboa com o título «Plano de Implementação da Norma ISO/IEC 27001 no INEM» (Correia, 2016).
- Muñoz apresenta em 2018 na Universidad Nacional Abierta y a Distancia na Colômbia uma tese de mestrado intitulada «Diseño de un SGSI Basado en la Norma ISO 27001 para la Empresa MA PEÑALOSA CÍA. S.A.S» (Muñoz, 2018).
- Sá Martins efetua em 2020 no Instituto Universitário de Lisboa uma tese que desenvolve um estudo intitulado «Visualization of Security in Industrial Control Systems respecting IEC-62443» (Sá Martins, 2020).

Contribuição para a estruturação do SIG do grupo Cooprofar

A Dissertação de (Oliveira, 2015) foi realizada no contexto empresarial do Grupo Cooprofar - Medlog que desenvolve as suas atividades de negócio na distribuição de medicamentos, como operador logístico. Pretende apresentar um caso de estudo sobre a estruturação do Sistema Integrado de Gestão (SGI), existente, da Qualidade (ISO 9001) com a inclusão da Gestão de Segurança da Informação ISO/IEC 27001, sendo que a implementação do sistema resultante é suportada no modelo de integração “Genérico, flexível, integrador, evolutivo e lean”.A dissertação é composta por 5 capítulos:

- Introdução:
  Onde é realizado um enquadramento do trabalho, os objetivos e resultados esperados, abordagem da investigação, metodologias de trabalho e estrutura do documento;
- Apresentação do grupo empresarial.
- Apresentação da literatura:
  Referenciais normativos de sistemas de Gestão (SGs) em utilização no Grupo, Sistemas Integrados de Gestão (SIGs), relevando as motivações e vantagens. Apresentação do modelo de integração considerando a inclusão do subsistema de Gestão de segurança da informação focado na ISO/IEC 27001.
- Caso de estudo e proposta de estruturação do atual sistema integrado de gestão do grupo.
- Conclusões e contributos.

Além dos principais objetivos, esta dissertação identifica desde logo alguns resultados esperados como: Proposta de estruturação da atual configuração de SIG da Qualidade, Inovação e Responsabilidade Social; Identificação de potenciais vantagens e ganhos de eficiência organizacional e de controlo de riscos em resultado da operacionalização e integração dos quatro sistemas de Gestão do modelo adotado "genérico, flexível, integrador, evolutivo e lean para SIGs"; identificação de desafios futuros resultantes da adoção e implementação de normas e subsistemas propostos.

Plano de Implementação da Norma ISO/IEC 27001 no INEM

Correia, efetua a preparação para a implementação de um SGSI inserido em ambiente Organizacional nomeadamente na Instituição INEM, baseado nas orientações da família de normas ISO/IEC 27000. Faz uso de vários processos específicos de modo a responder aos requisitos da ISO/IEC 27001:2013.

Este dá ênfase à caracterização teórica de um sistema de gestão da informação (SGSI) e a sua relevância no contexto e dinâmica da organização, no impacto com os sistemas e das tecnologias da informação e *framework* documental dos normativos necessários para gestão da segurança da informação, estrutura de recursos e responsabilidades.

No fundo, o documento representa a "primeira pedra" para a construção do sistema de gestão de segurança da informação que apresenta através da "Declaração de Aplicabilidade" conjunto de propostas subdivididas em cinco eixos de ação: Organizacional, Pessoal, Tecnológico, Físico e Ambiental, Legal & Regulatório. Para cada eixo de ação estão definidas medidas específicas a implementar e em consonância com os objetivos da organização INEM, de acordo com os requisitos das normas ISO/IEC 27001 e ISO/IEC 27002 (Correia, 2016).

Diseño de un SGSI Basado en la Norma ISO 27001 para la Empresa MA PEÑALOSA CÍA. S.A.S

Muñoz, desenha um sistema de segurança da Informação (SGSI) que contribui para a melhoria contínua dos ativos de TI na organização selecionada por si, mantendo sob controlo os risco que possam ser expostos por diversos fatores, sendo eles intencionais ou não intencionais, de origem física ou lógica, ambientais ou industriais. Durante o documento faz uma boa identificação dos ativos críticos, realiza a análise e gestão de risco através da metodologia MAGERIT recorrendo ao ciclo PDCA e efetua os respetivos controlos em conformidade com o normativo ISO/IEC 27001.

No final apresenta uma proposta de um SGSI que estabelece políticas e diretrizes para proteger ativos de TI que permite mitigar riscos e vulnerabilidades que possam afetar o normal funcionamento das operações de negócio (Muñoz, 2018).

Visualization of Security in Industrial Control Systems respecting IEC-6244

Sá Martins, implementa um sistema de visualização de eventos de segurança em sistemas de controlo industriais (ICS) recorrendo à série de normas de segurança IEC-62443.

Apresenta um estudo em parceria com a multinacional Siemens cujo objetivo é auxiliar na gestão de segurança de ICS identificando e mitigando de forma simplificada eventuais problemas do sistema. Recorre à avaliação de diversas ferramentas e plataformas para modelar e criar elementos visuais que representam componentes de um ICS com os

respetivos atributos de segurança, mostrando os resultados obtidos de forma simples e clara em dashboards (Sá Martins, 2020).

Motivos da Seleção

Os dois primeiros documentos Correia (2016) e Oliveira (2015) são distintos, pois o Oliveira (2015) enquadra-se num mestrado de Gestão de sistemas da informação e o Correia (2016) num mestrado em Engenharia e gestão industrial. O motivo para escolher duas áreas distintas é o facto de ambas proporcionarem pontos de vista distintos, mas complementares sobre o tema SGSI e pelo facto de(Oliveira, 2015) tentar integrar o SGSI abordando a ISO/IEC 27001 na norma ISO 9001 e por acrescentar a visão industrial, característica comum em muitas organizações.

O documento Muñoz (2018) oferece uma ampla visão sobre a implementação de um SGSI encontra-se muito bem explicado, implementa os controlos da norma ISO/IEC 27001, descreve políticas e procedimentos que podem ser adotadas em qualquer organização. Por fim apresenta as descobertas e propostas de mitigação dos resultados obtidos pela implementação do SGSI evidenciando o ciclo PDCA.

Por último, o documento Sá Martins (2020) acrescenta outro vetor de segurança que se tenta implementar neste documento, segurança em sistemas de controlo industriais (ICS) recorrendo à série de normas de segurança IEC-62443, os ICS estão amplamente implementados no ambiente produtivo da EIB a disrupção destes componentes poderá significar um grave prejuízo para toda a organização.

2.7 SÍNTESE

Neste capítulo, apresentou-se um Sistema de Gestão de Segurança da Informação (SGSI) e as etapas que o compõem, realizou-se um estudo abrangente sobre as normas e metodologias que se relacionam com o tema. Este exercício teve como objetivo estabelecer uma base sólida de conhecimento para a posterior implementação do SGSI.

O Centro Nacional de Cibersegurança (CNCS) promove e divulga as competências necessárias para que uma organização se torne segura no ambiente cibernético. Para

empresas que não necessitam de um sistema pesado, existe a opção de obter selos digitais que atestam a sua segurança. No entanto, para muitas organizações é importante mostrarem aos seus clientes e parceiros que estão conforme um standard amplamente reconhecido, como a ISO/IEC 27001.

Neste capítulo, foram também examinados outros casos de uso provenientes de trabalhos relacionados com a implementação de um SGSI, destacou-se também a importância das leis e regulamentos, como o RGPD e a Lei do Cibercrime.

3

CARATERIZAÇÃO DO CASO DE USO

Empresa Industrial de Borracha, S.A (EIB) é uma empresa portuguesa de transformação de borracha estabelecida em 1989, destaca-se no mercado devido à sua vasta experiência no setor e ao uso de matérias-primas de alta qualidade. Com tecnologia atualizada e altos padrões de qualidade, a EIB ocupa uma posição proeminente na indústria de materiais de recauchutagem, no fornecimento de compostos para pneus novos e em outros setores que dependem da borracha como matéria-prima principal.

Para dar cumprimento às constantes exigências dos seus principais clientes, sobretudo das empresas multinacionais do sector dos pneus implementou um sistema de gestão da qualidade e do ambiente, com a certificação do produto denominado piso pré-vulcanizado, com o qual abastece o mercado nacional e internacional. Adicionalmente, conta com um registo na EMAS - Sistema Comunitário de Ecogestão e Auditoria, visando afirmar a sua política de trabalhar com os melhores métodos e processos de fabrico, ambientalmente sustentáveis.

A empresa encontra-se sediada na Zona industrial da Marinha Grande, conta atualmente com cerca de 150 colaboradores e o seu volume de faturação situa-se aproximadamente nos 20 milhões de euros.

Ao longo dos seus mais de 30 anos de história, a EIB tornou-se uma referência nacional e internacional na fabricação de pisos e compostos de borracha para a indústria mundial de pneus, em concreto para as marcas Goodyear, Continental, Bridgestone e também para empresas de recauchutagem.

Cerca de 90% da produção é destinada ao mercado externo, e através das marcas mencionadas acima, os seus produtos chegam a diferentes mercados como Espanha, França, Alemanha, países do Leste e até ao Médio Oriente.

3.1 ORGANOGRAMA

Nesta secção, será apresentado o organograma da EIB na figura 21, que é uma representação visual da estrutura organizacional da empresa. O organograma é uma ferramenta importante para entender a hierarquia, as relações de autoridade e as responsabilidades dentro da EIB. Fornece uma visão clara dos diferentes níveis de gestão, departamentos e equipas, permitindo compreender como a EIB está organizada para atingir os seus objetivos.

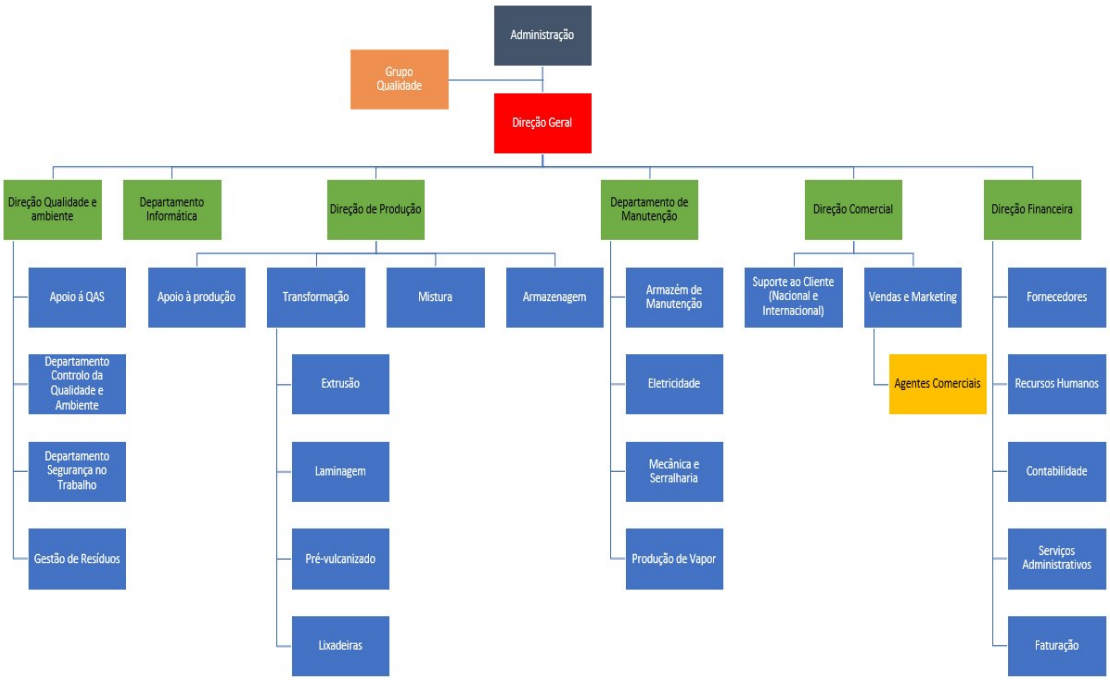


Figura 21: Organograma funcional da EIB

3.2 SISTEMA DE GESTÃO INTEGRADA

A EIB é uma organização certificada nas normas ISO 9001 e ISO 14001, e possui um registo no EMAS (Sistema Comunitário de Ecogestão e Auditoria). Estas certificações e registo são um reflexo do compromisso da EIB com a qualidade dos seus processos e com a gestão ambiental.

A certificação ISO 9001 estabelece os requisitos para um sistema de gestão da qualidade, garantindo que a EIB possui processos eficientes e eficazes para atender às necessidades dos seus clientes. Significa com isso que a EIB tem um compromisso com a excelência operacional, visando melhorar continuamente a qualidade dos seus produtos e serviços.

Já a certificação ISO 14001 estabelece os requisitos para um sistema de gestão ambiental. Ao obter essa certificação, a EIB demonstra o seu compromisso em identificar, monitorizar e controlar os impactos ambientais das suas atividades, procurando minimizar a sua pegada no meio ambiente e promover a sustentabilidade.

Além disso, a EIB também possui um registo no EMAS, que é um sistema voluntário de gestão ambiental, esse registo confirma que a EIB realiza auditorias ambientais periódicas, envolve os colaboradores e partes interessadas na gestão ambiental, promovendo a transparência e a responsabilidade ambiental.

Estas certificações e o registo no EMAS são reconhecidos internacionalmente e demonstram o compromisso da EIB com a qualidade, gestão ambiental e sustentabilidade. Conquistas que reforçam a posição da EIB como uma organização confiável, que procura a excelência nos seus processos e contribui para a preservação do meio ambiente.

3.3 RELAÇÃO ENTRE DEPARTAMENTOS E TECNOLOGIAS DE INFORMAÇÃO

Os sistemas de informação desempenham um papel fundamental no funcionamento, desenvolvimento e inovação de qualquer organização, isso é especialmente evidente na EIB. Como fabricante de produtos de borracha para a indústria de pneus e recauchutagem, a EIB depende em muito do trabalho realizado em cada departamento e das tecnologias de informação (TI) para garantir a normalidade dos seus processos.

A relação entre departamentos e sistemas de informação é crucial para o desenvolvimento das atividades diárias na EIB. Para se perceber essa relação, a Figura 22 apresenta um diagrama que ilustra as dependências existentes entre os departamentos e os sistemas de informação.

O diagrama demonstra como cada departamento está interdependente, sendo suportado pelas tecnologias de informação, para executar tarefas diárias e alcançar objetivos definidos.

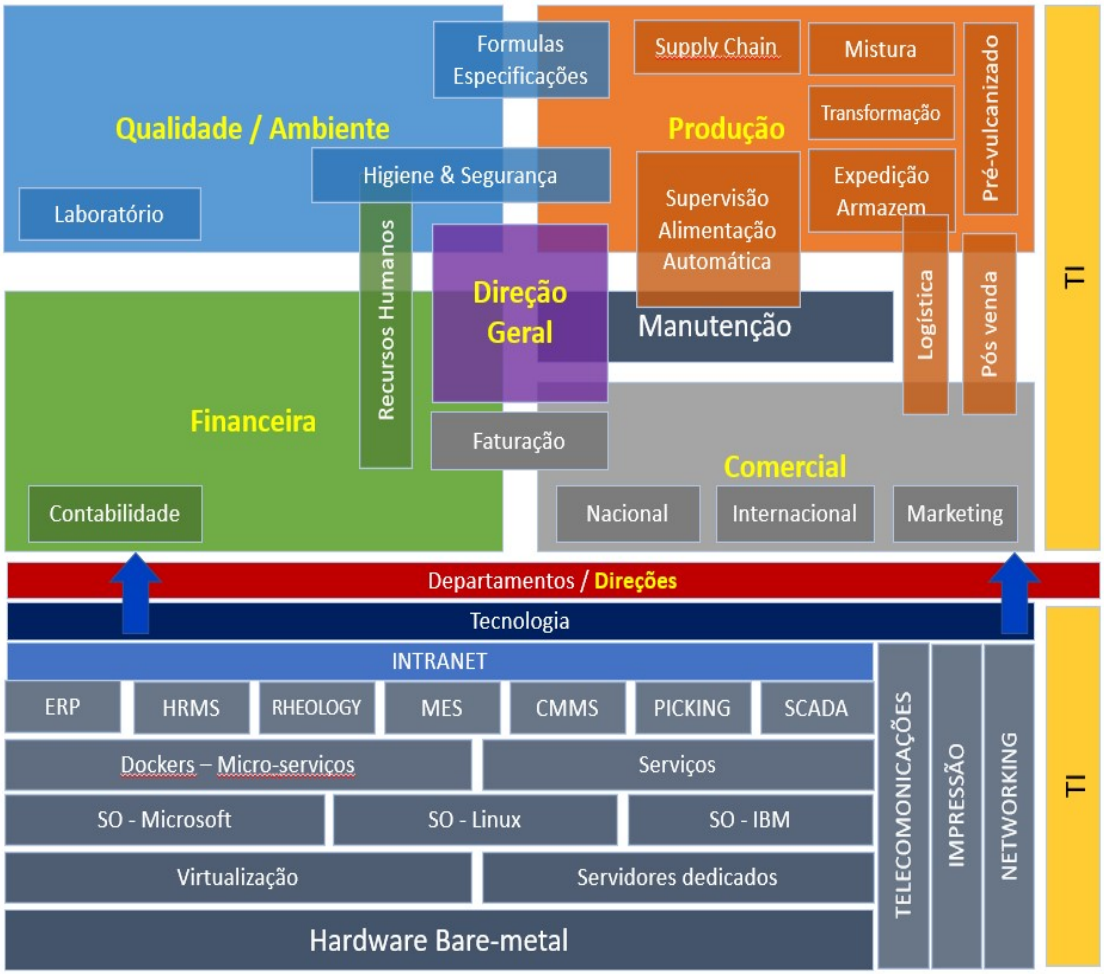


Figura 22: Diagrama dependências departamentais e TI

Através dos sistemas de informação, os departamentos podem partilhar informações, colaborar de maneira eficiente, automatizar processos e aceder a recursos essenciais para as suas operações.

No diagrama também é ilustrada a presença de diversas tecnologias aplicacionais, as quais serão descritas na seguinte lista:

- **ERP (Enterprise Resource Planning)**
  Software de gestão integrado existente na EIB para gerir processos Comerciais, Contabilísticos, Recursos humanos Financeiros, Produtivos, Inventários, entre outros.

- **HRMS (Human Resource Management System)**
  Software de gestão de recursos Humanos.
- **RHEOLOGY**
  Software laboratorial para gestão de teste de reologia, tensão, atrito, densidade, desgaste, entre outros.
- **MES (Manufacturing Execution System)**
  Software para fazer a gestão, planeamento, etiquetagem, recolha de dados da produção, pesagem, controlo de qualidade e dimensional do processo produtivo.
- **CMMS (Computerized Maintenance Management System)**
  Software para fazer a gestão de manutenção da empresa.
- **PICKING**
  Sistema de mobilidade utilizado para realizar atividades como receção de mercadorias, expedição, inventários, localizações e rastreabilidade.
- **SCADA Supervisory Control and Data Acquisition**
  Sistema monitorização, controlo e aquisição de dados em tempo real de processos industriais.

3.4 COMPONENTES TECNOLÓGICOS DE TI

A EIB possui um ecossistema de TI diversificado e abrangente, composto por vários componentes tecnológicos que desempenham um papel fundamental nas operações da organização. Em conjunto, esses componentes tecnológicos formam um ecossistema de TI complexo e interconectado. A gestão adequada desses elementos é fundamental para garantir a segurança, a disponibilidade e a eficiência dos sistemas de informação, bem como para suportar as operações e os objetivos estratégicos da EIB, a Figura 23 esquematiza o ecossistema de componentes de TI da EIB.

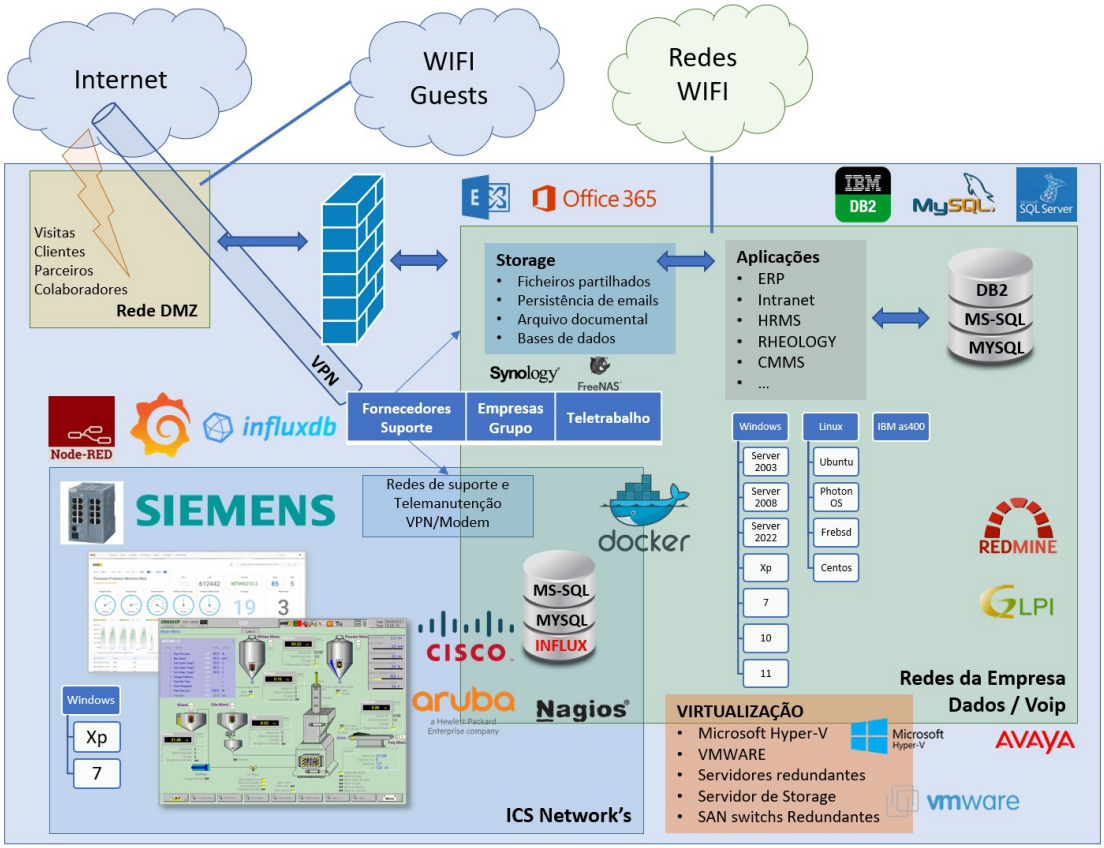


Figura 23: Heterogeneidade de componentes tecnológicos

Os principais aspetos dos componentes existentes no ecossistema da EIB incluem:

1. **Heterogeneidade de sistemas**

   Variedade de sistemas, que podem ter diferentes fornecedores, versões e arquiteturas. Esta heterogeneidade pode surgir devido a atualizações tecnológicas, integração de sistemas de terceiros ou aquisição de novas soluções. Gerir efetivamente esta diversidade de sistemas é essencial para garantir a interoperabilidade e a eficiência das operações.

2. **Diversidade de fluxos de informação**

   Ampla gama de fluxos de informação, que envolvem a troca de dados entre diferentes áreas, unidades de negócio, parceiros do grupo e clientes. Estes fluxos de informação podem ser estruturados ou não estruturados.

3. **Segregação de redes**

   Segregação de redes para garantir a separação adequada entre os diferentes ambientes de TI. Desta forma é necessário assegurar a criação de redes separadas para finalidades específicas, como redes internas, redes de acesso remoto, redes de convidados, redes de controlo industrial, entre outras. Esta abordagem contribui para o controlo de acesso e a redução do risco de comprometimento.

4. **Redes industriais**

   Devido à natureza da EIB, é comum a presença de redes industriais que suportam os sistemas de controlo e automação dos processos produtivos. Estas redes possuem requisitos específicos de segurança, confiabilidade e disponibilidade, exigindo a implementação de controlos adequados para proteger os ativos críticos e garantir a disponibilidade das operações.

5. **Redes Wi-Fi**

   As redes Wi-Fi fornecem conectividade sem fio aos seus colaboradores, clientes e visitantes. Essas redes permitem acesso à Internet, partilha de recursos e mobilidade dentro das instalações da organização. No entanto, é fundamental implementar medidas de segurança adequadas, como autenticação, criptografia e segregação de redes, para proteger os dados e mitigar riscos de segurança.

6. **Elevado número de soluções tecnológicas**

   A EIB utiliza uma variedade de soluções tecnologias no seu ecossistema de TI, incluindo servidores, sistemas de armazenamento, equipamentos de rede, dispositivos móveis, aplicativos empresariais, entre outros. A gestão eficaz destas soluções é essencial para garantir a estabilidade, o desempenho e a segurança dos sistemas de informação.

7. **Virtualização**

   A EIB utiliza tecnologias de virtualização para otimizar a utilização de recursos de TI e simplificar a administração de sistemas. A virtualização permite criar ambientes virtuais isolados, nos quais múltiplas instâncias de sistemas operativos e aplicativos podem ser executadas, proporcionando flexibilidade, escalabilidade e economia de custos.

8. **Heterogeneidade de sistemas operativos**

   No ecossistema da EIB existe uma grande variedade de sistemas operativos, como

Windows, Linux, As400, entre outros. Essa heterogeneidade decorre das necessidades específicas de cada aplicação ou plataforma. Gerir adequadamente esta diversidade de sistemas operativos é essencial para garantir a compatibilidade, estabilidade e segurança do ambiente de TI.

9. **Trabalho remoto e telemanutenção:**
   A EIB adota práticas de trabalho remoto e telemanutenção, permitindo que os colaboradores e fornecedores acedam aos sistemas de TI de forma segura e diferenciada, independentemente da localização geográfica. Esta abordagem oferece flexibilidade e contribui para a continuidade das operações, especialmente em situações de contingência ou falhas de equipamentos industrias.

10. **Componentes aplicacionais**
    A EIB utiliza uma variedade de aplicativos e sistemas de software para suportar as atividades operacionais, administrativas e estratégicas. Esses componentes aplicacionais já foram referidos na secção Relação entre Departamentos e Tecnologias de Informação. É fundamental garantir a integridade, a confidencialidade e a disponibilidade desses aplicativos para manter a eficiência e a competitividade da organização.

3.4.1 *Componentes desatualizados ou obsoletos*

A EIB enfrenta como muitas organizações o desafio de ter nos seus sistemas componentes de software e hardware desatualizados ou obsoletos "legados"que desempenham um papel crucial nas operações da empresa. Esses componentes são frequentemente utilizados em ambientes industriais, controlam máquinas e equipamentos específicos, no entanto, devido à sua antiguidade e à falta de suporte dos fabricantes, muitas vezes não é viável ou possível realizar atualizações.

A manutenção destes sistemas ou componentes é essencial para garantir a continuidade das operações, uma vez que eles desempenham um papel fundamental no controlo de processos industriais, também representam desafios significativos em termos de segurança e integração com outros sistemas mais recentes. Terão de ser implementados controlos de segurança adicionais para proteger estes sistemas contra ameaças cibernéticas, uma vez que muitas vezes não possuem as mesmas medidas de segurança que se podem

encontrar nos sistemas mais recentes e podem estar sujeitos a vulnerabilidades e ameaças de segurança, devido à falta de atualizações e suporte contínuo.

A gestão dos sistemas legados requer uma abordagem especializada, envolvendo ações como monitorização contínua, implementação de medidas compensatórias de segurança, isolamento desses sistemas de outras partes do ambiente de TI e consideração de estratégias de migração ou substituição a longo prazo. A EIB terá de encontrar um equilíbrio entre a necessidade de manter a funcionalidade dos sistemas legados e garantir a segurança e a continuidade dos processos industriais.

Trabalhar com sistemas legados é um desafio comum em muitas organizações que operam em ambientes industriais, onde a longevidade e a confiabilidade dos sistemas de controlo são críticas. Deve ser adotada uma abordagem cuidadosa para garantir a eficácia, segurança e a compatibilidade destes sistemas dentro do ecossistema de TI.

3.4.2 *Camada de apresentação - Intranet*

A EIB possui uma camada de apresentação web, denominada Intranet, que desempenha um papel fundamental na organização. Esta Intranet possui várias características importantes que contribuem para a eficiência e integração dos sistemas aplicacionais da EIB, descrevendo de seguida algumas das principais características da Intranet da EIB:

1. **Integração do portfólio aplicacional**
   Integração dos dados produzidos pelo portfólio de aplicações utilizadas pela empresa, desta forma os utilizadores podem aceder mediante a devidas autorizações, interagir e explorar os dados gerados por meio de uma única plataforma, facilitando o trabalho e a colaboração entre os diversos departamentos.
2. **Geração de relatórios e análise de dados**
   A Intranet da EIB oferece recursos para gerar relatórios e análise de dados permitindo que os utilizadores visualizem e interpretem informações relevantes para as suas atividades, auxiliando a tomada de decisões com base em dados concretos e atualizados.

3. **Suprimento de lacunas nas aplicações operacionais**
   A equipa de TI faz recurso da Intranet para preencher eventuais lacunas ou limitações nas aplicações operacionais. Desta forma disponibiliza funcionalidades adicionais ou complementares às aplicações principais, melhorando a experiência do utilizador e fornecendo recursos extras para atender às necessidades específicas da EIB.

4. **Painéis de controlo (dashboards)**
   Inclui dashboards personalizáveis, onde são apresentados indicadores, métricas e informações relevantes. Estes painéis permitem que os utilizadores acompanhem o estado dos processos, identifiquem tendências e visualizem dados de forma clara, intuitiva e integrada.

5. **Rastreabilidade**
   Como ponto central de integração de várias plataformas e aplicações, a intranet torna-se o local ideal para executar a importante tarefa de rastreabilidade, papel crucial em indústrias do setor químico. Desta forma a intranet implementa e apresenta uma rastreabilidade total do produto fabricado desde a aquisição de matérias-primas até aos processos de transformação e condições das máquinas envolvidas.

6. **Arquivo digital**
   A Intranet também atua como um arquivo digital, permitindo que os utilizadores armazenem, organizem, associem e partilhem documentos e informações importantes, contribuindo para a centralização e fácil acessibilidade dos dados, facilitando a colaboração e a consulta de informações relevantes.

   O Arquivo digital está plenamente alinhado com a estratégia de desmaterialização de papel, um dos objetivos estabelecidos pela EIB. A sua implementação representa um avanço significativo no sentido de eliminar progressivamente a dependência de documentos físicos e adotar uma abordagem mais sustentável e eficiente.

7. **Alertas**
   Possui um motor de alertas, que permitem notificar os utilizadores sobre eventos importantes, prazos, atualizações de dados ou qualquer outra informação relevante. Manter os utilizadores informados garante que eles recebam as informações necessárias oportunamente e que fiquem alertados sobre eventos relevantes para as suas atividades diárias.

8. **Desenvolvimento interno**
   Foi desenvolvida internamente pela equipa de TI, possibilitando que a solução seja escalável, adaptada às necessidades específicas da EIB e que ofereça recursos personalizados que atendam aos requisitos do negócio.

9. **Ambiente Web responsivo**
   Ambiente adaptado para dispositivos móveis, permitindo o acesso e a utilização da plataforma em diferentes dispositivos, como smartphones e tablets, proporcionando maior flexibilidade e conveniência aos utilizadores, que podem aceder à Intranet e utilizar as suas funcionalidades de forma eficiente em qualquer lugar e em qualquer momento.

A Intranet desempenha um papel fundamental na centralização, integração e melhoria dos processos e sistemas da organização. Com as suas características e funcionalidades, oferece uma plataforma abrangente para que os utilizadores acedam a informações integras e atualizadas, permitindo que tomem decisões conscientes e eficientes nas atividades que desempenham diariamente.

3.5 SÍNTESE

Neste capítulo, foi apresentado o caso de estudo nomeadamente a Empresa Industrial de Borracha, S.A. (EIB), objeto do projeto de implementação do Sistema de Gestão de Segurança da Informação (SGSI). Foram apresentados detalhes sobre a sua localização geográfica, principais clientes, mercados, volumes de faturação e número de colaboradores. Destacou-se o seu enquadramento enquanto indústria química, focada na produção de borracha para pneus e recauchutagem, apresentou-se a sua estrutura organizacional e as certificações obtidas, incluindo ISO 9001 e ISO 14001, bem como o registo no EMAS.

Posteriormente, foi explorada a grande interdependência entre os diferentes departamentos e em especial o departamento de TI, assim como as diversas tecnologias e softwares aplicacionais, dando destaque aos vários componentes tecnológicos que integram o ecossistema de Tecnologias de Informação (TI) da EIB.

Foi também abordado o grande desafio que representam os sistemas legados em ambientes industriais, seguindo a análise da camada de apresentação "Intranet", esta

camada integra e explora todos os softwares aplicacionais num ambiente web unificado, contribuindo para uma leitura fluida, integrada e coesa de todos os dados gerados na EIB.

4

IMPLEMENTAÇÃO

"O estabelecimento e implementação de um sistema de gestão de segurança da informação de uma organização são influenciados pelas necessidades e objetivos da organização, pelos requisitos de segurança, pelos processos organizacionais utilizados e pela dimensão e estrutura da organização" (*ISO/IEC 27001* 2013).

A implementação de um Sistema de Gestão de Segurança da Informação (SGSI) é uma etapa essencial para as organizações que procuram proteger de forma efetiva e eficaz os seus ativos de informação.

Neste capitulo serão apresentadas as principais fases na implementação de um SGSI, passando pelo suporte da gestão de topo, o âmbito, integração com os outros standards, definição de políticas e procedimentos e culminando com declaração de aplicabilidade.

4.1 SUPORTE DA GESTÃO DE TOPO

É fundamental que a direção esteja comprometida em liderar e promover a segurança da informação na organização, a fim de estabelecer uma cultura de proteção dos ativos de informação e garantir a continuidade dos negócios de forma segura.

A **cláusula 5.1** da ISO/IEC 27001 e **etapa 1 da fase de preparação** do roadmap da Integrity, estabelece os requisitos para o envolvimento da gestão de topo na implementação e manutenção do Sistema de Gestão de Segurança da Informação (SGSI). Para que a EIB esteja conforme esta cláusula, é necessário que a gestão de topo:

1. Demonstre compromisso
   A gestão de topo deve demonstrar um compromisso claro com a segurança da informação, estabelecendo uma cultura de segurança e fornecendo os recursos necessários para o SGSI.

2. Defina uma política de segurança
   A gestão de topo deve desenvolver, aprovar e comunicar uma política de segurança da informação que estabeleça os objetivos gerais de segurança e mostre o apoio da direção.
3. Integre a segurança da informação
   A gestão de topo deve assegurar que a segurança da informação seja integrada nas práticas de negócio da EIB, considerando a segurança nas decisões estratégicas e operacionais.
4. Comunique e consciencialize
   A gestão de topo deve comunicar e promover a consciencialização sobre a importância da segurança da informação em todos os níveis da organização, por meio de formações, campanhas de consciencialização e comunicações adequadas.
5. Faça revisões periódicas
   A gestão de topo deve rever periodicamente o desempenho do SGSI para garantir a eficácia e conformidade, e fornecer recursos para melhorias contínuas.

Com o objetivo de reforçar o compromisso da gestão de topo com a implementação do SGSI, a EIB optou por realizar uma auditoria de diagnóstico antes do início efetivo do projeto. Essa auditoria foi conduzida por uma empresa de consultoria especializada, seguindo as diretrizes e requisitos da norma ISO/IEC 27001.

A auditoria de diagnóstico teve como propósito realizar uma avaliação abrangente do estado atual da segurança da informação na EIB, identificando lacunas e áreas que requerem melhorias. Através dessa análise, foi possível estabelecer um ponto zero, que servirá como base para a implementação do SGSI.

A partir dos resultados da auditoria de diagnóstico, a EIB terá uma visão clara das áreas que requerem ações prioritárias e investimentos para melhorar a segurança da informação. Esta abordagem baseada em evidências e conforme com as práticas estabelecidas pela ISO/IEC 27001 permitirá que a EIB desenvolva um SGSI eficaz e adaptado às suas necessidades. O Resultado dessa auditoria pode ser consultado no apêndice E.

4.2 REUNIÕES DE KICKOFF

As reuniões de arranque marcam o início do projeto de implementação do SGSI e têm o objetivo de alinhar e consciencializar todas as partes interessadas, estabelecer metas e objetivos do projeto, definir as responsabilidades de cada membro e criar um plano de ação para a implementação do SGSI.

Estas reuniões são enquadradas na **cláusula 7** da ISO/IEC 27001 e **etapa 3 da fase de preparação** do roadmap da Integrity.

Foram efetuadas duas reuniões de arranque que contaram com a participação da gestão de topo, direção de qualidade, departamento de TI e direção de produção. Durante estas reuniões, foram abordados diversos temas relacionados com a implementação do SGSI na EIB, incluindo a definição do âmbito, a integração do SGSI nos sistemas de gestão já existentes, bem como a definição de algumas políticas a serem implementadas, como a política geral do SGSI. Foram ainda estabelecidas as responsabilidades e obrigações das partes interessadas no âmbito do SGSI.

4.3 ÂMBITO DO SGSI

Segundo o sítio da SGS entidade portuguesa de certificadora em diversas normas, inclusivamente a ISO/IEC 27001. A implementação de um Sistema de Gestão da Segurança da Informação (SGSI) requer um planeamento adequado, considerando o seu âmbito de aplicação, a integração com os sistemas existentes e a participação das partes interessadas relevantes.

O Requisito da norma ISO/IEC 27001 **4.3** determina que *"A organização deve determinar os limites e a aplicabilidade do sistema de gestão de segurança da informação para estabelecer o seu âmbito"*.

O âmbito do SGSI é também um documento entregável da **etapa 2 da fase de preparação** do roadmap da Integrity.

O âmbito de aplicabilidade do SGSI da EIB, definido na Política Geral de Segurança da Informação, abrange todas as informações, sistemas e equipamentos, independentemente

da sua localização ou forma de processamento, incluindo tanto as informações físicas como eletrónicas.

4.4 JUSTIFICAÇÃO DE SELEÇÃO DA NORMA ISO/IEC 27001

A decisão da EIB de adotar a ISO/IEC 27001 como norma principal do seu Sistema de Gestão de Segurança da Informação (SGSI) baseia-se em várias razões estratégicas e operacionais. Em primeiro lugar, como empresa europeia, a EIB reconhece a importância de alinhar as suas práticas de segurança da informação com normas internacionalmente reconhecidas. A ISO 27001 oferece um conjunto abrangente de diretrizes amplamente aceites na Europa e em todo o mundo.

Adicionalmente, a EIB já possui experiência e familiaridade com as normas ISO, como evidenciado pelas suas certificações na ISO 9001 e 14001, essa experiência prévia facilita a implementação da ISO/IEC 27001.

A decisão também é motivada pela necessidade de atender às expectativas e requisitos dos clientes da EIB, a maioria dos quais está localizada na Europa. A ISO/IEC 27001 é amplamente reconhecida e respeitada por organizações europeias, o que pode aumentar a confiança dos clientes na capacidade da EIB em proteger os seus dados e informações sensíveis.

4.5 INTEGRAÇÃO COM OUTROS PADRÕES

A integração de normas e standards é um fator importante a ser considerado na análise do impacto da certificação ISO/IEC 27001 no desempenho das organizações. Muitas organizações já implementam e estão conformes com outras normas, como a ISO 9001 ou a ISO 14001. No entanto, adotar várias normas independentemente umas das outras pode exigir um esforço significativo à organização.

Para evitar duplicação de tarefas, documentação, funções e estruturas, uma solução é desenvolver um sistema de gestão integrado com diferentes normas, permitindo que o conhecimento acumulado de um standard seja aplicado noutro, não apenas a nível operacional, mas também na integração de processos de gestão do risco Su. et al. (2015).

Calder, 2009 refere que organizações que já possuem um sistema conforme com a ISO 9001 podem simplesmente estendê-lo para incluir um SGSI, pois este será capaz de obter certificação de acordo com a ISO 27001. A nota da **cláusula 1.2** "Aplicação"da ISO/IEC 27001 reconhece isso:

"If an organization already has an operative business process management system (e.g. in relation with ISO 9001 or ISO 14001), it is preferable in most cases to satisfy the requirements of this International Standard within this existing management system."

A integração de diferentes normas permite ainda que as competências organizacionais sejam fortalecidas, melhorando assim a competitividade e o desempenho do sistema de gestão.

A literatura existente identifica diversos vetores de similaridades entre diversas normas ISO, incluindo a ISO/IEC 27001, e destaca os benefícios da integração de processos de gestão do risco centralizados e integrados. Em suma, a integração da norma ISO/IEC 27001 com outros standards pode trazer benefícios significativos às organizações, incluindo melhorias na posição de mercado e no seu desempenho organizacional.

4.5.1 *Partes interessadas*

Para cumprir o requisito da **cláusula 4.2**, nomeadamente o controlo 5.31 da norma ISO/IEC 27001:2022, é necessário identificar as partes interessadas e os seus requisitos para o SGSI. A EIB já possui um documento que identifica as partes interessadas no sistema de gestão existente, que deve ser utilizado para adicionar as entidades relevantes para o SGSI.

Entre as partes interessadas que devem ser consideradas, estão as entidades reguladoras, tal como a Comissão Nacional de Proteção de Dados (CNPD) e o Centro Nacional de Cibersegurança (CNSC). É importante também identificar os requisitos das partes interessadas, como os clientes que exigem confidencialidade dos dados e fornecedores relevantes de tecnologia ou serviços.

Ao preencher o documento existente no sistema de gestão da EIB com estas entidades e requisitos relevantes, a EIB garante que todas as partes interessadas pertinentes sejam

consideradas, permitindo uma maior abrangência na gestão da segurança da informação, atendendo às expectativas e necessidades das partes interessadas envolvidas.

Ao compreender e atender aos requisitos das partes interessadas, a EIB estabelece relações de confiança, assegurando a proteção adequada das informações, processo que contribui para a conformidade com a norma ISO/IEC 27001 e reforça a segurança da informação da EIB.

4.5.2 *Ações de formação e consciencialização em SI*

A conformidade com a norma ISO/IEC 27001 **cláusulas 7.2 e 7.3** exige que a EIB inclua ações de formação nas áreas de segurança da informação nos seus planos de formação. O objetivo dessas ações de formação é garantir que todos os colaboradores se sintam confortáveis ao utilizar as ferramentas de tecnologia da informação (TI) no seu dia a dia, além de os consciencializar para os perigos do mundo digital e os riscos que podem afetar as operações da EIB caso não sigam as políticas estabelecidas.

É essencial que os colaboradores estejam familiarizados com as melhores práticas de segurança da informação e que compreendam os potenciais perigos do mundo digital e através da formação serão consciencializados dos riscos associados ao uso inadequado ou negligente dos recursos de TI, bem como das consequências que essas ações podem ter para a EIB.

A formação contínua em segurança da informação garante que os colaboradores estejam atualizados sobre as políticas e diretrizes estabelecidas pela EIB, permitindo que apliquem as melhores práticas nas suas atividades diárias e tomem decisões conscientes, alinhadas com as políticas de segurança da EIB.

4.5.3 *Comunicação*

No âmbito da **cláusula 7.4** da norma ISO/IEC 27001, está estabelecida a necessidade de desenvolver um plano de comunicação, tanto interna como externa, relativo à segurança da informação. Este plano inclui a comunicação de incidentes de segurança da informação, riscos identificados, estratégias de resposta a incidentes e outras informações pertinentes.

Este plano já está integrado no sistema de gestão existente na EIB, encontrando-se dividido entre comunicações internas e externas. O plano identifica objetivos específicos, as partes interessadas envolvidas, os responsáveis pela comunicação, a frequência e os meios de comunicação a serem utilizados, que abrangem reuniões, quadros informativos, correio eletrónico, telefone, inquéritos, entre outros. Este documento será revisto para incluir os requisitos das 4.5.1 partes interessadas definidas na norma ISO/IEC 27001. A figura 24 demonstra as alterações cirúrgicas realizadas no plano de comunicações da EIB para contemplar os requisitos de comunicação da ISO/IEC 27001.

Tipo	Objectivo (O que comunicar)	Destinatários (A quem comunicar)	Responsável (Quem comunica)	Meios/ Suportes (Como comunicar)	Frequência (Quando comunicar)
Interna	Nova legislação com impacto no SGQA e SI ou alteração a existente	Responsáveis dos Departamentos, conforme aplicável	DQA, DSI	Reuniões internas	Sempre que existam
	Entrada/saída de colaboradores	Responsáveis dos Departamentos, conforme aplicável	Serviço de Pessoal, DSI	Mail	Sempre que existam
	Não conformidades detectadas na Produção e/ou CQ e tambem de SI	Responsáveis dos Departamentos, conforme aplicável	DP, CCQA, DQA	Mail, reuniões	Sempre que existam
	Resultados de Auditorias Internas e Externas, componente de SI	Responsáveis dos Departamentos, conforme aplicável	DQA	Mail, reuniões	Sempre que existam
	Incidentes de Segurança da Informação	Gestão de topo,Responsaveis de departamentos, Colaboradores	DSI	Mail, telefone, my.eib.pt, reuniões internas	Sempre que existam
	Politica e procedimentos de SI	Colaboradores	DSI	Mail, Quadro informativo	Sempre que existam novos ou alterações
	Políticado SGSI	Colaboradores	DSI	Mail, Quadro informativo	Sempre que existam
Externa	Política da Qualidade e Ambiente	Clientes, Parceiros, Fornecedores e Outras Partes Interessadas Externas	DQA	Site da EIB	Contínuo
	Medição grau de satisfação dos Clientes	Clientes	Resp. Marketing	Inquérito de opinião	Anual
	Requisitos de prestação dos serviços	Fornecedores de Serviços	DG, DQA, DP, DM ou DAC	Mail	Sempre que Necessário
	Requisitos de matérias primas	Fornecedores de Matérias Primas	DG, DQA, DP ou DAC	Mail	Sempre que Necessário
	Embalagens importadas para consumo próprio	APA	DQA	Site APA	Anual:até 31 de Março
	Emissões gasosas	CCDR Centro	DQA	Carta registada com AR	Oxidação 2x/ano;caldeira e lixadeira 3 em 3 anos
	Descarga de águas residuais	CMMG	DQA	Carta registada com AR	Anual
	Registo de Produtores/embaladores	APA	DQA	Site APA	Anual: Até 31 de Março
	Incidentes de Segurança da Informação	CNSC	DSI	Site CNSC	Sempre que se verifiquem
	Incidentes de Segurança da Informação com fuga de dados pessoais	CNPD, CNSC	DSI	Site CNPD, site CNSC	Sempre que se verifiquem

Figura 24: Plano comunicações EIB

4.5.4 *Riscos e oportunidades*

Conforme a **cláusula 6.1** da norma ISO/IEC 27001, é necessário ter em consideração os riscos e oportunidades de segurança da informação. Assim, com o objetivo de integrar esses elementos nos sistemas de gestão existentes na EIB, serão considerados adicionalmente os itens identificados abaixo, na análise SWOT já existente na EIB:

- **Riscos (Ameaças)**
  1. Risco de perda de propriedade intelectual
     a possibilidade de roubo, acesso não autorizado ou divulgação indevida de informações confidenciais, como fórmulas químicas, processos de fabricação e projetos de produtos.
  2. Risco de perda de dados de clientes
     Ameaça de violação de dados, que pode resultar em perda de informações pessoais ou financeiras de clientes, impactando com a confiança e a reputação da EIB.
  3. Risco de interrupção das operações
     Possibilidade de interrupção dos sistemas de TI, seja devido a falhas técnicas, ataques cibernéticos ou desastres naturais, resultando em paralisação das atividades de produção.
  4. Risco de não conformidade regulatória
     Ameaça de não cumprimento das regulamentações aplicáveis à indústria, como a proteção de dados pessoais, requisitos de segurança específicos do setor ou legislação comunitária.
- **Oportunidades**
  1. Implementação de medidas de segurança acessíveis
     Oportunidade de adotar soluções de segurança da informação adequadas à dimensão e recursos da EIB, como antivírus, firewalls e backups regulares, para proteger as informações e minimizar os riscos.
  2. Melhoria dos controlos de segurança física
     Oportunidade de implementar medidas adicionais de segurança, como monito-

rização por câmaras, controlo de acesso físico e proteção contra incêndio, para proteger as instalações e os ativos da EIB.

3. Fortalecimento da confiança dos clientes e parceiros comerciais
   Oportunidade de demonstrar que a empresa possui medidas robustas de segurança da informação, aumentando a confiança dos clientes e parceiros comerciais na qualidade e confiabilidade dos produtos e das informações partilhadas.
4. Consciencialização e treino dos colaboradores
   Oportunidade de promover a educação e a consciencialização dos colaboradores sobre as boas práticas de segurança da informação, reduzindo os riscos associados a erros humanos e criando uma cultura de segurança.
5. Parcerias com fornecedores confiáveis
   Oportunidade de estabelecer parcerias com fornecedores de TI confiáveis e especialistas em segurança para obter suporte e soluções adequadas às necessidades da empresa.
6. Revisão e melhoria contínua
   Oportunidade de realizar avaliações regulares de risco e revisões do sistema de gestão de segurança da informação, visando identificar áreas de melhoria e implementar ações corretivas e preventivas.

4.5.5 *Análise SWOT*

A análise SWOT é uma ferramenta amplamente utilizada para avaliar a situação atual de uma organização, identificar pontos fortes e fracos internos, bem como oportunidades e ameaças externas. Na implementação da norma ISO/IEC 27001, a análise SWOT pode servir para avaliar o ambiente de segurança da informação e identificar áreas que precisam de ser fortalecidas ou melhoradas.

Ao considerar a certificação ISO 9001 já existente na EIB, a análise SWOT pode ser realizada em conjunto com a implementação da ISO/IEC 27001 para obter uma visão abrangente da gestão de qualidade, ambiente e segurança da informação na organização.

Alguns pontos de verificação associados à segurança da informação e relacionados com a análise SWOT além dos identificados na secção 4.5.4 podem incluir:

1. **Pontos fortes (Strengths)**
    - Identificar os recursos, competências e processos existentes na organização que contribuem para a segurança da informação.
    - Analisar as vantagens competitivas da EIB em termos de segurança da informação relativamente a outras organizações do mesmo setor.
    - Avaliar as práticas de gestão de qualidade já implementadas na EIB que podem ser aproveitadas para a implementação da ISO/IEC 27001.
2. **Pontos fracos (Weaknesses)**
    - Identificar as áreas de fraqueza em relação à segurança da informação na organização, como lacunas na gestão de riscos, falta de consciencialização dos colaboradores sobre segurança da informação, ou sistemas de TI desatualizados.
    - Avaliar os desafios específicos que a EIB pode enfrentar na implementação da ISO/IEC 27001, como restrições orçamentais ou resistência à mudança.
3. **Oportunidades (Opportunities)**
    - Identificar oportunidades de melhoria na segurança da informação, como a adoção de novas tecnologias ou a melhoria dos processos de gestão de riscos.
    - Explorar possíveis parcerias ou colaborações que possam fortalecer a segurança da informação da EIB.
4. **Ameaças (Threats)**
    - Identificar as ameaças atuais ou emergentes que podem afetar a segurança da informação da EIB, como ataques cibernéticos, regulamentações mais rigorosas ou avanço tecnológico que podem tornar as soluções existentes obsoletas.

Ao realizar essa análise SWOT na implementação da ISO/IEC 27001 em conjunto com a certificação ISO 9001, a EIB poderá identificar os principais desafios e oportunidades relacionados com segurança da informação e definir estratégias eficazes para melhorar os sistemas de gestão de qualidade, ambiente e segurança da informação.

4.6 GESTÃO DOCUMENTAL

A gestão documental desempenha um papel fundamental na implementação e manutenção de um SGSI é requisito na **cláusula 7.5** da ISO/IEC 27001 sob o título de "Documentação de suporte"e um entregável da **etapa 1 da fase de preparação** do roadmap da Integrity. Nesse sentido, a EIB aproveita as sinergias já estabelecidas na implementação de outros sistemas de gestão, como a ISO 9001 e a ISO 14001 para otimizar a gestão documental, garantindo a conformidade com os requisitos da ISO/IEC 27001.

Com esta abordagem sinérgica, a EIB utiliza os conhecimentos e recursos já adquiridos na implementação da ISO 9001 e 14001 para estabelecer políticas e procedimentos eficazes no que diz respeito à criação, revisão, aprovação, controlo, distribuição e arquivamento de documentos de segurança da informação.

Esta estratégia não aumenta apenas a eficiência e a consistência na gestão documental, mas também facilita a conformidade com as normas e padrões de segurança estabelecidos.

4.6.1 *Objetivos*

Atualmente a EIB define no seu procedimento de gestão documental os seguintes objetivos que serão a seguir adaptados ao SGSI:

- Definir linhas de orientação para a elaboração dos documentos do Sistema de Gestão da EIB;
- Descrever o método utilizado para permitir o controlo da distribuição dos documentos, para garantir que os utilizadores dispõem da versão atualizada da documentação, bem como de que são utilizadas as versões atualizadas dos impressos;
- Definir o modo como é garantido o controlo dos registos necessários para garantir a operação eficaz e o controlo do Sistema da Qualidade, Ambiente e **Segurança da Informação** . Estes registos podem servir também para proporcionar evidências de conformidade com os requisitos (relativamente a normas, a regulamentação ou a disposições definidas no quadro deste Sistema de Gestão da Qualidade, Ambiente e **Segurança da Informação**).

4.6.2 *Fluxograma*

No âmbito do presente projeto, foi realizada uma adaptação no fluxograma da gestão documental com o intuito de incorporar as medidas de segurança da informação, essa modificação pode ser visualizada na figura 25.

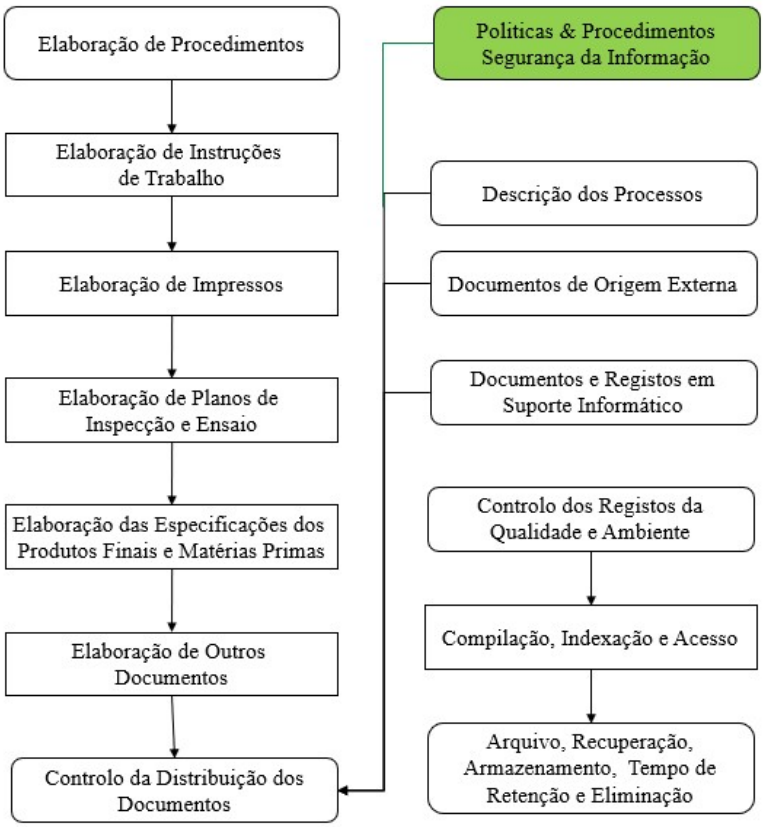


Figura 25: Fluxograma documental da EIB

4.6.3 *Políticas e procedimentos de SI*

No âmbito do procedimento de gestão documental da EIB, foi criada uma nova secção com o propósito de definir a estrutura necessária para as políticas e procedimentos de Segurança da Informação.

4.6.3.1 *Políticas de SI*

As políticas de Segurança da Informação (SI) são diretrizes estabelecidas pela EIB para definir as práticas e comportamentos necessários para garantir a segurança das informações, estabelecem os princípios, responsabilidades e regras que devem ser seguidas pelos colaboradores relativamente à proteção e uso adequado das informações, visam mitigar riscos, garantir a confidencialidade, integridade e disponibilidade dos dados, além de promover a conformidade regulatória e a cultura de segurança na EIB.

Politicas

Os documentos de políticas de Segurança da Informação, com um âmbito mais amplo, adotam o seguinte formato de estrutura:

- Introdução;
- Âmbito;
- Responsabilidades;
- Diretrizes;
- Conclusão.

A estrutura apresentada não é fixa, podendo ser adaptada para atender às necessidades específicas da EIB.

Políticas de uso Aceitável

No que diz respeito às políticas de uso aceitável, direcionadas principalmente aos utilizadores de sistemas de informação, seguem uma estrutura ligeiramente diferente, que é descrita a seguir:

- Alcance / Aplicabilidade;
- Propósito;
- Política;
- Manutenção da Política;

- Exceções;
- Sanções.

Também neste caso a estrutura não é fixa podendo ser alterada para atendar as especificidades da política.

4.6.3.2 *Procedimentos*

Os procedimentos de Segurança da Informação consistem em instruções detalhadas que orientam a implementação e execução de medidas de segurança específicas, descrevem os passos e ações a serem seguidas para garantir a proteção das informações e sistemas da EIB. Assumem a finalidade de estabelecer diretrizes claras e padronizadas para garantir a segurança e integridade dos ativos de informação da EIB.

Os procedimentos de SI deverão seguir a seguinte estrutura que pode ser adaptada conforme as necessidades específicas do procedimento:

- Objectivo;
- Âmbito;
- Responsabilidades;
- Procedimentos;
- Medidas de controlo;
- Documentação relacionada;
- Conclusão.

4.6.4 *Outras secções*

No âmbito do procedimento de gestão documental da EIB, serão realizadas alterações em várias secções para incluir os domínios do Sistema de Gestão de Segurança da Informação (SGSI). Algumas dessas secções que serão modificadas são as seguintes:

1. Identificação e Classificação de Documentos
   Será incluída a classificação dos documentos conforme os domínios do SGSI, para garantir a devida proteção e confidencialidade da informação.
2. Armazenamento e Preservação
   Serão estabelecidas diretrizes específicas para o armazenamento seguro dos documentos relacionados com domínios do SGSI, garantindo a sua integridade e disponibilidade.
3. Controlo de Versões
   Será implementado um sistema de controlo de versões para os documentos relacionados com Segurança da Informação alinhado com o já existente na EIB, assegurando que apenas as versões atualizadas e aprovadas estejam em circulação.
4. Acesso, Distribuição e Controlo de Documentos
   Serão definidos os procedimentos de acesso e controlo dos documentos relacionados com o SGSI, estabelecendo níveis apropriados de autorização e restrições para garantir a segurança da informação.
5. Revisão e Atualização de Documentos
   Serão estabelecidos prazos e responsabilidades claras para a revisão e atualização dos documentos relacionados com o SGSI, assegurando a sua conformidade contínua com as políticas e normas estabelecidas.

Estas alterações visam integrar adequadamente os domínios do SGSI no procedimento de gestão documental da EIB, proporcionando uma gestão eficiente e segura dos documentos relacionados com a segurança da informação.

4.6.5 *Responsabilidades documentais*

A elaboração de documentos na EIB segue uma hierarquia estabelecida, na qual cada indivíduo ou departamento desempenha um papel específico. A organização procura definir um circuito para a criação de documentos relacionados com os seus sistemas de gestão.

Esse circuito envolve a identificação das necessidades de documentação, a designação de responsáveis pela elaboração dos documentos, a revisão e aprovação pelas partes

interessadas e finalmente, o arquivo adequado dos documentos. Desta forma, a EIB assegura que os documentos sejam criados de acordo com padrões e requisitos estabelecidos, garantindo a consistência e a qualidade das informações documentadas.

A imagem 26 apresentada abaixo define um excerto das responsabilidades associadas à elaboração, verificação, aprovação e arquivo dos documentos do Sistema de Gestão adaptada à Segurança da Informação da EIB:

Documentos	Elaboração	Verificar	Aprovar	Arquivo
Manual de Gestão	DQA	ADM	ADM	DQA 2 anos
Fichas de Processo	R. Processo	GQA	ADM	DQA 2 anos
Procedimentos	R. Processo	GQA	R. Processo	DQA 2 anos
Instruções de Trabalho	Chefes de Departamento	GQA	DQA	DQA 2 anos
Descrição de Funções	DQA	DQA	DG	DQA 2 anos
Política de SI	DSI	DSI	ADM	DSI 3 anos
Formulações e Especificações da Mistura	DTI	DSI	DSI	DSI 2 anos
Formulações/Especificações de Produto Final	DTI	DSI	DSI	DSI 2 anos

Figura 26: Responsabilidades de elaboração, aprovação e arquivo de documentos do SIG EIB

A título de exemplo, na imagem 26, o documento "Política de SI"é elaborado e verificado pelo Departamento de Segurança da Informação (DTI), aprovado pela Administração (ADM), arquivado pelo DTI e deve ser revisto a cada 3 anos.

4.7 MANUAL DE FUNÇÕES

O Manual de Funções desempenha um papel essencial no contexto do Sistema de Gestão de Segurança da Informação (SGSI) da EIB. Estabelece as responsabilidades e autoridades

relacionadas com as funções de TI na organização, garantindo a conformidade com a ISO/IEC 27001.

O requisito **5.3** da norma ISO/IEC 27001, intitulado **"Funções, Responsabilidades e Autoridades na Organização"**, estipula que "a gestão de topo deve assegurar a atribuição e comunicação das responsabilidades e autoridades para as funções relevantes no âmbito da segurança da informação", para obter informações mais detalhadas, a norma ISO/IEC 27003 desempenha o papel de contribuir para a definição das responsabilidades e cargos relacionados com gestão de segurança da informação.

O manual será revisto e atualizado regularmente para garantir a sua relevância e conformidade contínua com as necessidades e os requisitos de segurança da informação da EIB.

Propósito

O manual de funções da EIB pretende estabelecer claramente as responsabilidades e autoridades relacionadas com as funções de TI na organização. Visa fornecer orientações claras sobre as responsabilidades individuais, promover a eficiência operacional e garantir a segurança e integridade dos recursos de TI.

Âmbito

Este manual de funções abrange as principais funções relacionadas com gestão das tecnologias da informação na EIB e é aplicável a todos os colaboradores e departamentos envolvidos nas atividades de TI, desde a gestão estratégica até a administração e suporte dos sistemas.

Descrição de Funções

1. Responsável pela Segurança da Informação

- Encarregado de supervisionar e coordenar a estratégia de segurança da informação da EIB;
- Desenvolve políticas, procedimentos e práticas de segurança da informação para proteger ativos e dados;
- Realiza avaliações regulares de risco e análises de vulnerabilidade para identificar potenciais ameaças;
- Coopera com os diversos departamentos para implementar e manter medidas de segurança;
- Monitoriza continuamente ameaças e tendências de segurança para ajustar as medidas de proteção conforme necessário;
- Participa em auditorias relacionadas com a segurança da informação;
- Assegura que todos os colaboradores estejam cientes das políticas e práticas de segurança da informação mediante formações e ações de consciencialização.

2. Diretor de TI

- Responsável pela estratégia e a direção geral da área de TI;
- Define políticas e procedimentos relacionados com a segurança e uso dos recursos de TI;
- Supervisiona as operações de TI e assegura o alinhamento com os objetivos organizacionais;
- Garante a proteção dos dados e ativos da organização, implementando medidas de segurança adequadas e promovendo a cultura de segurança;
- Aplica medidas para assegurar o acesso lógico e físico aos ativos de informação;
- Supervisiona a gestão, manutenção e otimização da infraestrutura de TI, redes e sistemas, assegurando a disponibilidade e o desempenho;
- Gere parcerias e contratos com fornecedores de TI, avaliando soluções e garantindo a qualidade dos serviços contratados;
- Promove a adoção de tecnologias emergentes e processos inovadores para melhorar a eficiência e eficácia dos processos de negócios;

- Colabora com outras áreas da organização para identificar oportunidades de melhoria, resolver desafios e promover a integração de sistemas.

3. Administrador de Sistemas
    - Responsável pela administração e manutenção dos sistemas e infraestrutura de tecnologia da informação;
    - Monitoriza o desempenho dos sistemas e realiza atualizações e manutenções conforme necessário;
    - Gere contas de utilizadores e as suas permissões de acesso aos sistemas.
4. Analista de Segurança da Informação
    - Responsável pela análise e avaliação dos riscos de segurança da informação;
    - Desenvolve e implementa medidas de segurança para proteger os dados e sistemas da organização;
    - Implementa e monitoriza sistemas de gestão centralizada de logs;
    - Realiza auditorias de segurança e investigações de incidentes de segurança.
5. Administrador de Bases de Dados
    - Responsável por gerir as bases de dados da EIB;
    - Garante a integridade, segurança e disponibilidade dos dados;
    - Realiza backups e recuperação de dados em caso de falhas;
    - Colabora com a equipa de segurança da informação na aplicação de medidas de proteção dos dados.
6. Programador
    - Responsável pela criação e manutenção de software para a EIB;
    - Desenvolve soluções conforme os requisitos de negócio e as diretrizes de segurança;
    - Implementa boas práticas de programação para garantir código seguro e livre de vulnerabilidades;

- Colabora com a equipa de segurança da informação na análise e correção de vulnerabilidades.

7. Suporte Técnico
    - Responsável por fornecer suporte técnico aos utilizadores e resolver problemas relacionados com hardware e software;
    - Instala, configura e mantém os dispositivos e softwares utilizados;
    - Fornece orientação e formação sobre o uso adequado dos recursos de TI;
    - Garante a conformidade com as políticas de segurança da informação ao fornecer suporte;
    - Colabora com a equipa de segurança da informação na deteção e resposta a incidentes de segurança;
8. Administrador de Rede
    - Responsável pela configuração e gestão da infraestrutura de rede;
    - Monitoriza o tráfego de rede, realiza análises de desempenho e implementa melhorias conforme necessário;
    - Garante a segurança e integridade da rede, implementando medidas de proteção contra ameaças externas;

4.8 ANÁLISE GAP

Segundo Al-Mayahi e Sa'ad (2012) A análise de GAP é um processo que consiste em comparar os controlos implementados por uma organização com os definidos pela norma ISO/IEC 27001. A análise GAP ou análise de lacunas em português é uma ferramenta, ou técnica que permite à organização verificar o seu desempenho real relativamente aos padrões estabelecidos. É importante salientar que a análise GAP difere da avaliação de riscos, uma vez que se concentra na comparação do objeto relativamente a um objetivo específico, como um nível de desempenho desejado ou uma norma, ao passo que a avaliação de riscos não é medida relativamente a um objetivo específico. Tanto a análise GAP como

a avaliação de riscos visam fornecer uma resposta à pergunta "onde estamos?", mas, no caso da análise GAP, essa resposta é medida em relação a "onde queremos estar".

A análise GAP faz parte da **etapa 4 da fase de diagnóstico** do roadmap da Integrity e normalmente envolve as seguintes etapas:

1. Revisão dos requisitos de segurança:
   Os requisitos de segurança relevantes, como os da ISO/IEC 27001, são revistos e compreendidos.
2. Avaliação do estado atual
   A organização realiza uma avaliação detalhada da segurança da informação atual, examinando os controlos existentes, políticas, procedimentos e práticas de segurança implementados.
3. Identificação de lacunas
   Com base na comparação entre os requisitos e o estado atual, são identificadas as lacunas ou áreas onde a organização não está em conformidade, ou não atende totalmente aos requisitos de segurança da informação.
4. Elaboração do plano de ação
   Com base nas lacunas identificadas, é desenvolvido um plano de ação detalhado que descreve as medidas corretivas e as atividades necessárias para fechar as lacunas de segurança da informação.
5. Implementação das melhorias
   A organização executa o plano de ação, implementando as melhorias necessárias para alcançar a conformidade com os requisitos de segurança da informação.
6. Monitorização revisão contínua
   Após a implementação das melhorias, o SGSI é continuamente monitorizado e revisto para garantir a eficácia e a conformidade contínua.

Tendo em conta as características de uma análise de GAP, é necessário compreender o ponto de partida para identificar as discrepâncias e as alterações desejadas. Nesse sentido, a EIB decidiu contratar externamente uma auditoria de diagnóstico antes de implementar o seu Sistema de Gestão de Segurança da Informação (SGSI), cujos resultados podem ser consultados no apêndice E.

Uma vez que se trata de uma implementação a partir do zero, é natural que a maioria dos controlos da norma ISO/IEC 27001 não estejam implementados inicialmente. Será necessário desenvolver as políticas e procedimentos correspondentes para garantir que a organização esteja em conformidade com a norma. Nesse sentido, será realizada uma análise mais aprofundada no capítulo 5 Gestão de Riscos.

4.9 POLÍTICAS DE SEGURANÇA E PROCEDIMENTOS

4.9.1 *Políticas de Segurança da Informação*

Com o avanço crescente da tecnologia e o fácil acesso à informação, a segurança da informação tornou-se um tema crucial para empresas de todos os setores. A EIB reconhece a importância da proteção de informações sensíveis e está comprometida em garantir a segurança das suas informações mediante políticas e medidas de segurança.

As Políticas de Segurança da Informação são documentos fundamentais que visam garantir a proteção e a integridade dos ativos de informação da EIB, estas políticas estabelecem diretrizes e requisitos que devem ser seguidos por todos os colaboradores, contratados a fornecedores que tenham acesso aos sistemas e dados da organização.

A implementação de políticas de segurança eficazes é essencial para mitigar riscos, prevenir incidentes de segurança e promover uma cultura de proteção da informação. Estas políticas visam assegurar a confidencialidade, integridade e disponibilidade dos dados, bem como garantir a conformidade com as leis e regulamentos aplicáveis.

Alcance

O alcance das políticas de segurança da informação varia conforme a estrutura e necessidades da EIB. Em geral, a política deve abranger todas as informações sensíveis da empresa e ser aplicável a todos os colaboradores, funcionários, fornecedores e parceiros que tenham acesso a essas informações.

A política de segurança da informação deve ser implementada em todos os departamentos e áreas da EIB, incluindo tecnologia da informação, recursos humanos, financeira,

compras, produção, marketing, entre outros. É importante que todos os colaboradores estejam cientes da política e que sejam treinados para poderem aplicar a política nas suas atividades diárias.

Além disso, a política de segurança da informação pode ter um alcance mais amplo, abrangendo também os clientes, fornecedores e parceiros da EIB, que devem ser orientados a seguir as diretrizes de segurança ao lidar com as informações sensíveis da empresa.

Em resumo, o alcance de uma política de segurança da informação deve ser abrangente, o suficiente, para proteger todas as informações sensíveis da EIB e todos os colaboradores envolvidos no seu tratamento, garantindo a integridade, confidencialidade e disponibilidade dessas informações.

Sanções por não comprimento

A EIB encara a segurança da informação de forma muito a séria e entende que o não cumprimento das políticas de segurança da informação pode comprometer a integridade, confidencialidade e disponibilidade das informações sensíveis da empresa. Por isso, foram estabelecidas sanções claras e objetivas para quem não cumprir as diretrizes estabelecidas na política de segurança da informação.

As sanções podem incluir advertências formais, suspensão temporária do acesso às informações sensíveis da empresa, demissão por justa causa, entre outras medidas disciplinares aplicáveis, dependendo da gravidade da violação e do impacto na segurança da informação.

Cabe aos gestores e colaboradores da EIB garantir que as políticas de segurança da informação sejam cumpridas rigorosamente para evitar quaisquer sanções e proteger as informações sensíveis da empresa.

4.9.1.1 *Políticas Definidas*

No Apêndice A deste documento, estão definidas as políticas específicas que orientam a proteção, o uso adequado e a gestão da informação na EIB. Essas políticas são complementares às diretrizes gerais e devem ser seguidas por todos os colaboradores da organização. As políticas no Apêndice A abrangem os seguintes tópicos:

- A.1 Política Geral de Segurança da Informação;
- A.2 Política de Backups e Recuperação;
- A.3 Política de Rede;
- A.4 Política de Monitorização e Registo de Eventos;
- A.5 Política de Gestão de Ativos;
- A.6 Política de Acesso e Controlo de Informação;
- A.7 Política de Sensibilização e Formação em SI;
- A.8 Política de Desenvolvimento de Software;
- A.9 Política de Classificação da Informação;
- A.10 Política de Gestão e Eliminação de Suportes de Informação;
- A.11 Política de Controlo Criptográfico;
- A.12 Política de Controlo de Acessos Físicos;
- A.13 Política de Transferência de Informação;
- A.14 Política de Relação com Fornecedores;
- A.15 Política de Gestão de Riscos.

4.9.2 *Políticas de uso aceitável para recursos de TI*

As políticas de uso aceitável estabelecem orientações para o comportamento dos colaboradores ao utilizar os recursos tecnológicos da empresa, diferenciam-se das políticas gerais por serem mais direcionadas aos utilizadores dos sistemas. O objetivo é fomentar um uso ético e responsável, em conformidade com leis como o RGPD e normas como a ISO/IEC 27001.

A EIB procura criar um ambiente seguro e protegido para o uso de recursos tecnológicos, garantindo a privacidade dos indivíduos e os interesses da empresa. Todos, desde a gestão de topo até aos funcionários de todos os níveis hierárquicos, partilham a responsabilidade de cumprir estas políticas.

A adesão a estas políticas reforça a segurança da informação e dos ativos da empresa, promovendo um ambiente ético, é necessário que todos compreendam e sigam estas orientações para melhorar a consciencialização sobre práticas seguras no uso de tecnologia.

A EIB definiu as seguintes políticas de utilização aceitável, que estão detalhadas no Apêndice B:

- B.1 Leis e Normas;
- B.2 Papeis e Responsabilidades;
- B.3 Manutenção de Postos e Ambiente de Trabalho;
- B.4 Correio Eletrónico Empresarial;
- B.5 Navegação na Internet;
- B.7 Ética e Privacidade;
- B.8 Software e Licenças;
- B.9 Trabalho Remoto;
- B.10 BYOD (Bring Your Own Device);
- B.11 Gestão de Passwords;
- B.12 Segurança de Dados Pessoais;
- B.13 Incidentes de Segurança da Informação.

4.9.3 *Procedimentos de TI*

Os procedimentos de TI na estrutura da ISO 27001 complementam as políticas e são altamente detalhados, muitas vezes contendo instruções passo-a-passo para assegurar a consistência e a eficácia das operações., abrangem uma ampla gama de áreas na EIB, desde o registo de incidentes de segurança da informação até o controlo de acessos físicos e lógicos, incluindo sistemas de CCTV, VPNs e trabalho remoto. É essencial que esses procedimentos sejam desenvolvidos e implementados conforme os requisitos legais e normativos, visando garantir a proteção das informações e a conformidade com as melhores práticas de segurança cibernética, estes devem ser implementados e mantidos

por colaboradores com as competências e conhecimentos necessários para executar as tarefas. Estes são documentos entregáveis da **etapa 10 da fase de implementação** do roadmap da Integrity.

A seguir, apresentam-se os procedimentos atualmente em vigor na EIB, que abrangem diversas áreas. É relevante destacar que maioria destes procedimentos não está disponível em apêndice devido à sua natureza específica, que comprometeria a privacidade dos sistemas e processos da EIB:

- C.1 Operações com Utilizadores;
- C.2 Registo de incidentes de segurança da informação;
- Comunicação de eventos de segurança da informação;
- Gestor centralizado de passwords;
- Recuperação de passwords;
- Gestor de certificados;
- Inventario de ativos tecnológicos;
- Gestão de configurações;
- Backups integrais;
- Restauro de backups integrais;
- Backup e restauro de bases de dados;
- Controlo de acessos físicos instalações;
- Registo e visualização de imagens de CCTV;
- Sistema de alarmistica;
- Acessos remotos e VPN;
- Privilégios a aplicações operacionais;
- Privilégios a sistemas de ficheiros;
- Atualização dos sistemas operativos servidores Microsoft;
- Atualização de sistemas operativos desktop Microsoft;

- Contactar com as autoridades competentes para incidentes de segurança da informação.

Com efeito, o SGSI é uma estrutura dinâmica e adaptativa que deve evoluir em consonância com as necessidades e desafios em constante mudança. Sendo assim, a lista de procedimentos apresentada anteriormente não deve ser considerada rígida ou imutável, mas sim sujeita a revisões e atualizações periódicas.

4.9.4 *Síntese de Políticas e Procedimentos*

Na secção dedicada às "Políticas de Segurança e Procedimentos", foram abordados tópicos essenciais para a estruturação do ambiente de segurança da informação na EIB. As Políticas de Segurança da Informação fornecem o enquadramento e diretrizes para práticas de segurança, estabelecendo princípios e objetivos a serem seguidos por todos os colaboradores.

As Políticas de Uso Aceitável de TI visão estabelecer regras e limitações no uso dos recursos tecnológicos da empresa, garantindo a proteção dos ativos de informação e promovendo a conduta adequada dos utilizadores.

Os Procedimentos de TI detalham as etapas e instruções específicas para a execução de tarefas e operações de TI de forma segura e consistente, complementam as políticas, traduzindo-as em ações práticas a serem seguidas pelos colaboradores no seu dia a dia.

4.10 DECLARAÇÃO DE APLICABILIDADE (SOA)

A Declaração de Aplicabilidade (DA) também designada como SoA é um requisito obrigatório no processo de implementação da norma ISO/IEC 27001 nomeadamente a **Clausula 6.1.3.d** e um entregável da **etapa 11 da fase de implementação** do roadmap da Integrity, descreve a abordagem adotada pela organização relativamente aos controlos de segurança da informação especificados no Anexo A da norma. A DA é um documento estruturado que identifica os controlos aplicáveis e justifica a sua implementação, tendo em conta os riscos de segurança da informação enfrentados pela organização.

Através da Declaração de Aplicabilidade, a organização define quais os controlos que serão implementados e quais não serão aplicados, deve incluir justificações para a exclusão de controlos e fornecer informações adicionais sobre as medidas de segurança adotadas.

A Declaração de Aplicabilidade serve como uma ferramenta de comunicação interna e externa, permitindo que a organização demonstre o seu compromisso com a segurança da informação e a conformidade com os requisitos da ISO/IEC 27001, é um documento fundamental para garantir a consistência e a transparência na implementação dos controlos de segurança da informação, proporcionando uma visão clara do âmbito e das medidas de segurança adotadas pela organização.

A DA fornece informações sobre o estado de implementação de cada controlo da ISO/IEC 27001, ajudando a identificar lacunas e orientar as ações necessárias para alcançar a conformidade com a norma. A tabela da DA geralmente contém as seguintes colunas:

1. Identificação do controlo
   Número ou código que identifica cada controlo da ISO/IEC 27001.
2. Descrição do controlo
   Descrição do controlo específico da ISO/IEC 27001.
3. Estado de implementação
   Indica se o controlo está implementado, parcialmente implementado ou não implementado. No caso da tabela SoA da EIB esse estado é sempre o mesmo, pois trata-se de uma implementação de raiz onde todos os controlos estão na sua fase inicial.
4. Justificação
   Breve justificação para o estado de implementação do controlo ou a sua não aplicabilidade.
5. Referência documental
   Referências a documentos que suportam a implementação do controlo.
6. Responsável
   A pessoa ou função responsável pela implementação e manutenção do controlo. No caso da EIB será o Departamento de Segurança da Informação.

A Declaração de Aplicabilidade da EIB encontra-se apresentada no Apêndice D deste documento e realiza o mapeamento de todos os controlos aplicáveis e não aplicáveis do Anexo A da norma ISO/IEC 27001.

4.11 SÍNTESE

No capítulo de "Implementação", abordam-se vários tópicos para estabelecer um Sistema de Gestão de Segurança da Informação (SGSI) em conformidade com a norma ISO/IEC 27001, começando-se por obter suporte da gestão de topo e com a definição do âmbito do SGSI. Além disso, foi explorada a integração SGSI com outras normas e padrões, considerando as partes interessadas, ações de formação e sensibilização, a avaliação de riscos e oportunidades e a análise SWOT.

Neste capítulo, também são definidas as políticas e procedimentos que farão parte dos controlos aplicados na ISO/IEC 27001.

O capitulo destaca a importância da gestão documental para criar e manter procedimentos e políticas de segurança, bem como a elaboração do Manual de Funções para definir as responsabilidades de cada membro com funções de TI. Aborda a análise GAP, que compara os controlos existentes com os requisitos da ISO/IEC 27001.

Por fim, concluí-se com a elaboração da Declaração de Aplicabilidade (SoA), documento essencial e obrigatório da ISO/IEC 27001 que identifica os controlos selecionados para tratar os riscos e estar conforme os objetivos de segurança da informação da organização.

5

GESTÃO DE RISCOS

A gestão de riscos é um elemento essencial no âmbito da norma ISO/IEC 27001, que estabelece os requisitos para um SGSI. O objetivo principal da gestão de riscos na ISO/IEC 27001 é ajudar a organização a identificar, analisar e tratar os riscos relacionados com segurança da informação de forma eficaz.

A gestão de riscos no processo de implementação do SGSI da EIB seguirá a abordagem estabelecida na norma ISO/IEC 27005 e utilizará como referência o "Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança"do Centro Nacional de Cibersegurança.

5.1 METODOLOGIA GESTÃO DO RISCO

A metodologia de gestão de riscos adotada pela EIB segue uma abordagem sistemática para identificar, analisar, avaliar e tratar os riscos relacionados com segurança da informação. Esta metodologia é baseada nas melhores práticas estabelecidas na norma ISO/IEC 27005, é um entregável da **etapa 6 da fase de diagnóstico** do roadmap da Integrity e consiste nas seguintes fases como apresentado na figura 27 que representa o processo da gestão de riscos da ISO/IEC 27005:

1. Estabelecer contexto
   Definir os objetivos, estratégias, âmbito, fronteiras e parâmetros das atividades incluídas na gestão de riscos da organização, bem como os recursos necessários para a sua operacionalização.
2. Identificação de riscos
   São identificados os possíveis riscos que podem afetar a segurança da informação na organização, envolvendo uma análise completa dos ativos, ameaças e vulnerabilidades existentes.

3. Análise de riscos

   Os riscos identificados são analisados em termos da sua probabilidade de ocorrência e potencial impacto, permitindo priorizar os riscos e concentrar os esforços nos mais críticos.

4. Avaliação de riscos

   Os riscos são avaliados com base em critérios predefinidos, considerando a sua gravidade e a capacidade da organização em tratar deles, determinando dessa forma a necessidade de tratamento dos mesmos.

5. Tratamento de riscos

   Os riscos são tratados de acordo com estratégias definidas, que podem incluir a implementação de controlos de segurança, transferência de riscos ou a aceitação dos riscos. As ações de tratamento visam reduzir a probabilidade de ocorrência e minimizar o impacto dos riscos.

6. Monitorização e revisão

   A gestão de riscos é um processo contínuo. Os riscos identificados são monitorizados regularmente para garantir que os controlos implementados sejam eficazes. Além disso, a avaliação de riscos é revista periodicamente para se adaptar a novas ameaças, vulnerabilidades ou alterações no ambiente de negócios.

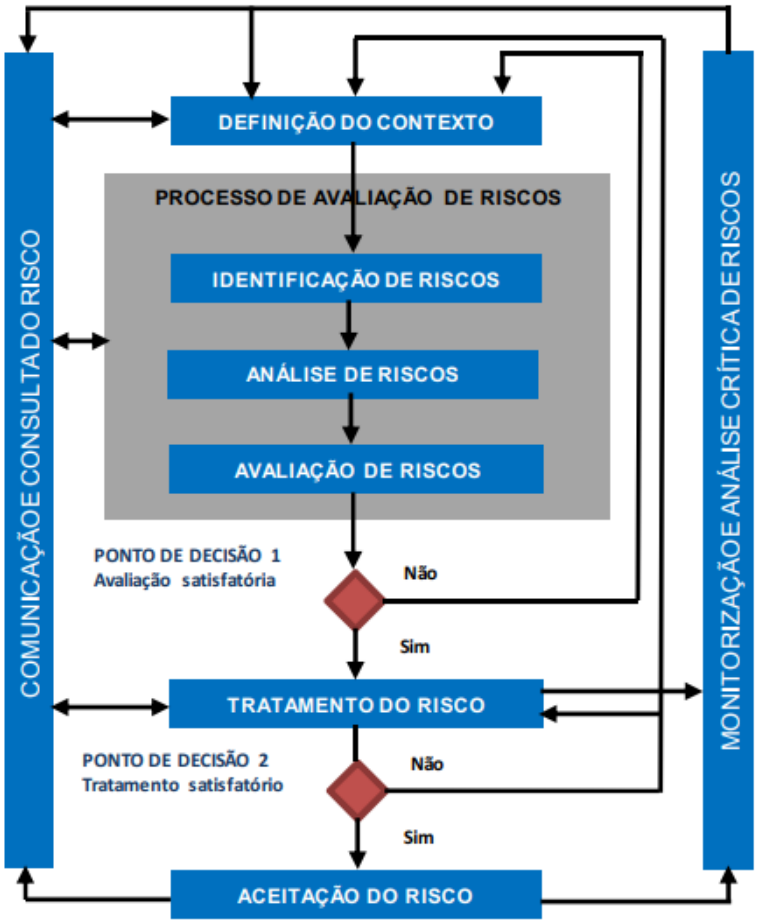


Figura 27: Processo de Gestão de Risco, adapatado de (*ISO/IEC 27005* 2022)

Através desta metodologia, a EIB procura garantir que a segurança da informação seja abordada de forma estruturada e abrangente, permitindo a tomada de decisões informadas e a implementação de medidas adequadas para proteger os seus ativos de informação contra ameaças internas e externas.

5.2 ESTABELECER O CONTEXTO

A fase de Estabelecer o Contexto no processo de gestão de riscos, desempenha um papel de relevo no planeamento e implementação desse processo, é através desta fase que se procura compreender os critérios, decisões, recursos e elementos internos e externos

relevantes para a organização, que possam influenciar a sua capacidade de alcançar os objetivos definidos.

Durante a fase inicial de Estabelecer o Contexto no processo de gestão de riscos, é importante que a organização identifique os recursos humanos como partes interessadas internas e/ou externas. É necessário definir as funções e responsabilidades relacionadas com a gestão de riscos de segurança da informação, incluindo:

1. **Gestão de Topo**
    - Analisar e aprovar todas as decisões tomadas no processo de gestão dos riscos;
    - Delegar funções dentro da organização no que diz respeito ao processo de gestão de risco.
2. **Gestor de Risco**
    - Controlar processo de gestão dos riscos da organização;
    - Assegurar que a recolha de toda a informação necessária para a identificação do risco é realizada;
    - Assegurar que toda a informação necessária para a análise é recolhida;
    - Assegurar a realização da análise dos riscos;
    - Assegurar que as opções escolhidas para tratar os riscos são as mais corretas;
    - Assegurar que o processo de gestão dos riscos se mantém compatível com a política, objetivos e com os demais requisitos legais e regulatórios aplicáveis à organização;
    - Assegurar que a framework interna da gestão de risco é comunicada a todos os colaboradores com funções relevantes para a sua aplicação.
3. **Dono do Risco**
    - Gerir ativos ou sistemas de informação e os seus respetivos riscos e participar no processo de gestão dos riscos;
    - Assegurar que o risco é reportado ao Gestor do Risco;
    - Assegurar que o risco é identificado, analisado, avaliado e tratado;
    - Assegurar que as opções de tratamento são cumpridas.

Além dos recursos humanos, é igualmente relevante identificar os recursos materiais necessários para garantir a execução eficaz do processo de gestão de riscos, incluindo a utilização de ferramentas de suporte apropriadas e a definição de processos adequados para o tratamento dos riscos.

Outra atividade importante nesta fase é a definição do âmbito e das fronteiras do processo de gestão de riscos, envolve estabelecer claramente quais as áreas, ativos ou processos que estão incluídos no âmbito do processo de gestão de riscos (Centro Nacional de Cibersegurança, 2023).

5.3 GESTÃO DE ATIVOS

A implementação bem-sucedida de um SGSI, seguindo as orientações da norma ISO/IEC 27001, está intrinsecamente ligada à gestão eficaz dos ativos. Esta prática envolve a identificação, classificação e proteção adequada dos ativos de informação da organização, com o intuito de assegurar a confidencialidade, integridade e disponibilidade desses ativos.

A gestão de ativos abrange diversos elementos, não se limitando apenas aos ativos de informação, mas também incluindo ativos físicos e tecnológicos, envolvendo uma série de atividades, como a definição de estratégias de classificação, a atribuição de responsabilidades aos proprietários, a implementação de medidas de segurança apropriadas e a mitigação dos riscos associados aos ativos de informação. O objetivo destas atividades é garantir uma proteção adequada dos ativos da organização contra ameaças internas e externas ou de outras naturezas, tais como fogos, inundações, catástrofes naturais, etc. A gestão de ativos também possibilita que as organizações protejam informações sensíveis, reduzam riscos e estejam em conformidade com requisitos regulatórios.

5.3.1 *Ativos*

No capítulo 3 da ISO/IEC 27001, intitulado "Termos e definições"é apresentada a definição de "Ativo"como "Qualquer coisa que tenha valor para a organização, incluindo os recursos de informação que suportam as operações e a continuidade do negócio". A norma também

define outros termos relacionados, como "Ativos de Informação", "Proprietário do Ativo"e "Responsável pelo Ativo".

Os ativos têm um papel significativo na operação e continuidade dos negócios de uma organização, sendo fundamental protegê-los de forma adequada. Estes podem ser classificados em diferentes categorias, como ativos tangíveis (materiais) e ativos intangíveis (informação). A identificação e classificação corretas dos ativos são fundamentais para perceber a sua importância, avaliar os riscos associados e implementar as medidas de segurança apropriadas.

Segundo o CNCS os ativos podem ter as seguintes categorias:

- Tecnológicos (hardware, software, dispositivos de rede e sistemas);
- Pessoas;
- Informação;
- Ambiente Físico e Localizações;
- Third Party - consistem nas dependências contratuais internas ou externas ao serviço.

5.3.2 *Classificação e valorização de ativos*

A determinação da criticidade, valorização ou classificação dos ativos deve ser baseada no impacto resultante de uma eventual falha, ou indisponibilidade para a organização, sendo o objetivo garantir que os ativos recebam um nível adequado de proteção, conforme a sua importância. Essa classificação pode considerar requisitos legais, valor financeiro, criticidade estratégica e sensibilidade das informações contidas no ativo, entre outros critérios relevantes. Alguns dos critérios de classificação de ativos incluem:

1. Valor Financeiro
   Podem ser classificados conforme o seu valor monetário para a organização, o valor pode ser determinado com base em fatores como custo de aquisição, custo de substituição, valor de mercado ou impacto financeiro em caso de perda ou comprometimento.

2. Valor Estratégico
   Podem ser classificados com base na sua importância estratégica, ativos com um papel crucial no cumprimento dos objetivos organizacionais, no suporte a processos críticos de negócios, etc.
3. Sensibilidade e Confidencialidade
   Podem ser classificados conforme o nível de sensibilidade ou confidencialidade das informações que contêm, avaliando a natureza e o grau de sigilo das informações manipuladas pelo ativo.
4. Disponibilidade
   Podem ser classificados com base na sua importância para a disponibilidade contínua dos serviços ou sistemas da organização.
5. Integridade
   Podem ser classificados com base na importância da integridade das informações que contêm.
6. Requisitos Legais
   Podem ser baseados nos requisitos legais e regulatórios aplicáveis à organização, esses requisitos podem estabelecer categorias específicas de classificação.

Uma abordagem interessante para avaliar os ativos com base nos três pilares da segurança da informação (CIA) é a fórmula apresentada pelo Centro Nacional de Cibersegurança, 2023 no seu guia de gestão de riscos de segurança da informação.

$$\textbf{Valor Ativo} = \textbf{Max(Confidencialidade; Integridade; Disponibilidade)}$$

5.3.3 *Ameaças e vulnerabilidades*

Uma ameaça é um evento ou circunstância, com o potencial de causar danos, perdas ou interrupções aos ativos de uma organização (*ISO/IEC 27001* 2013), é algo que representa um perigo ou risco para a segurança da informação e pode resultar em consequências indesejáveis. Exemplos de ameaças incluem ataques cibernéticos, desastres naturais, erros humanos, roubo físico, entre outros.

Uma vulnerabilidade, por outro lado, é uma fraqueza ou falha num sistema, processo ou controlo que pode ser explorada por uma ameaça para causar danos ou comprometer a segurança dos ativos (*NIST SP 800-53* 2020). É uma condição que facilita a ocorrência de um incidente de segurança, estas podem ocorrer devido a falhas de conceção, configurações inadequadas, falta de atualizações de segurança, políticas ou procedimentos ineficientes, entre outros fatores.

Em resumo, as ameaças são os eventos ou circunstâncias que podem causar danos, enquanto as vulnerabilidades são as fraquezas ou falhas que podem ser exploradas por essas ameaças, é importante identificar e gerir tanto as ameaças quanto as vulnerabilidades para proteger os ativos e garantir a segurança da informação.

5.3.4 *Inventários de ativos*

O inventário de ativos da EIB consiste numa lista detalhada de todos os recursos de informação considerados importantes e críticos para a organização, contém informações relevantes sobre cada ativo, como o seu tipo, localização, proprietário, responsável pela gestão, entre outros detalhes relevantes.

A finalidade do inventário de ativos é proporcionar uma visão abrangente dos recursos de informação da EIB, permitindo a identificação, classificação e gestão adequada destes ativos. Esta prática auxilia na proteção adequada das informações, na definição de medidas de segurança apropriadas e na tomada de decisões relacionadas com a gestão de riscos.

O inventário de ativos deve ser regularmente atualizado e revisto, garantindo a sua precisão e abrangência, sendo uma ferramenta essencial para o desenvolvimento e implementação de controlos de segurança adequados, assim como para a monitorização e melhoria contínua do Sistema de Gestão de Segurança da Informação (SGSI) da EIB.

O Inventário de ativos enquadra-se com a **cláusula 8.1** da ISO/IEC 27001 e com a **etapa 5 da fase de diagnóstico** do roadmap da Integrity.

Salienta-se que a EIB no âmbito deste projeto implementou uma solução tecnológica (GLPI) para realizar inventário de ativos de informação, gerir incidentes de SI e controlar configurações de equipamentos.

Apresenta-se abaixo a tabela 4 com um pequeno exemplo de inventário de ativos da EIB com as classificações e valorizações definidas nas secções acima, neste exemplo foram omitidos campos como a localização, tipo de ativo, proprietário, responsável, entre outros.

Codigo	**Ativo**	**Custo Finan.**	**Criticidade**	**Valor CIA**				**Acesso**
				C	**I**	**D**	**Val**	
HW.0001	Servidor	8 000 €	Muito	4	4	5	5	Restrito
SF.0001	Software RH	12 000 €	Crítico	5	5	3	5	Confidencial
CA.0001	Controlo de acessos arquivo físico	750 €	Pouco	3	1	3	3	Restrito
SP.0001	Projetor formação	1 500 €	Não	1	1	2	2	Publico
CA.0002	Relógio de ponto	900 €	Critico	4	4	4	4	Interno
INF.0001	Formulas compostos de clientes	– €	Extremo	5	5	3	5	Confidencial

Tabela 4: Exemplo inventario de ativos valorizado e classificado

5.4 AVALIAÇÃO DE RISCO

No contexto específico da segurança da informação, o risco refere-se à possibilidade de uma ameaça explorar vulnerabilidades num ativo ou conjunto de ativos, o que pode resultar em danos para o sistema. O risco é avaliado com base na probabilidade de ocorrência de um evento negativo, como a exploração de uma vulnerabilidade por parte de uma ameaça, e nas perdas ou prejuízos causados aos ativos (Correia, 2016). *"Um Sistema de Gestão de Segurança da Informação visa preservar a confidencialidade, integridade e disponibilidade das informações por meio da aplicação de um processo de gestão de riscos"* (*ISO/IEC 27001* 2013).

Assim, é crucial para a organização estabelecer e implementar um processo de gestão de riscos de segurança da informação que inclua a identificação e análise dos riscos, bem como a avaliação dos riscos de segurança da informação. A identificação dos riscos de segurança da informação é um dos primeiros passos para o desenvolvimento de um sistema de gestão de segurança da informação.

5.4.1 *Metodologia de avaliação de riscos*

A EIB utiliza atualmente no seu sistema de gestão ISO 9001 a fórmula "probabilidade (P) x impacto (I)" para calcular o risco. Esta fórmula é aplicada na avaliação dos riscos associados às atividades e processos da organização.

$$\textbf{Risco} = \textbf{P x I}$$

A probabilidade refere-se à possibilidade de ocorrência de um evento indesejado, enquanto o impacto representa as consequências desse evento nos objetivos e resultados da empresa. A EIB atribui valores numéricos numa escala de **1 a 5** para representar a probabilidade e o impacto.

Ao multiplicar a probabilidade pelo impacto, obtém-se um valor que representa o nível de risco, neste caso, a EIB estabeleceu um limite de **superior a 9** como critério para a definição e planeamento de ações. O que significa que sempre que o resultado do cálculo do risco for igual ou superior a 10, serão tomadas ações para mitigar ou controlar o risco identificado.

Ao utilizar o mesmo critério de avaliação de riscos da ISO 9001 para a ISO/IEC 27001, a EIB visa manter uma abordagem consistente na gestão de riscos em todas as áreas da organização, permitindo uma visão integrada e coerente dos riscos relacionados com a segurança da informação, garantindo uma gestão eficaz dos riscos em todas as suas atividades.

No âmbito do desenvolvimento deste projeto, a EIB utilizará o cálculo do impacto, levando em consideração os três pilares da segurança da informação: confidencialidade, integridade e disponibilidade (CIA), de forma a obter um resultado mais refinado. Sendo adotada uma abordagem ponderada, atribuindo pesos diferentes para cada uma das áreas: Para a confidencialidade, será atribuído um peso de 40%; para a integridade um peso de 30%; e para a disponibilidade um peso de 30%. Assim, a fórmula utilizada para calcular o impacto será a seguinte:

$$\textbf{Impacto} = \textbf{Confidencialidade x 0.4} + \textbf{Integridade x 0.3} + \textbf{Disponibilidade x 0.3}$$

Com esta abordagem, será possível avaliar de forma mais precisa o impacto nos diferentes aspetos da segurança da informação.

De seguida, será apresentada a tabela 5 categorias de classificação da probabilidade em vigor na EIB, adaptada para os riscos associados à segurança da informação [1].

Probabilidade	Descrição
Frequente (**5**)	Existem registos muito frequentes de ocorrência (mais de 12 por ano), como dados de outras entidades, reclamações de clientes, registos internos, etc., e é fortemente previsível que ocorra, tendo em conta as condições existentes. Incidentes de segurança de informação mais de um por mês.
Provável (**4**)	Existem registos frequentes de ocorrência (até 6 por ano), como dados de outras entidades, reclamações de clientes, registos internos, etc., e é bastante previsível que ocorra, tendo em conta as condições existentes. Incidentes de segurança de informação um por mês.
Possível (**3**)	Existem registos pontuais de ocorrência (até 3 por ano), como dados de outras entidades, reclamações de clientes, registos internos, etc., e é previsível que ocorra, tendo em conta as condições existentes. Incidentes de segurança de informação um a cada 6 meses
Improvável (**2**)	Não existem registos de ocorrência, mas é razoável a expectativa da ocorrência, tendo em conta as condições existentes. Incidentes de segurança de informação um a cada 2 anos.
Rara (**1**)	Não existem registos de ocorrência e não é previsível que ocorra. Incidentes de segurança de informação um a cada 5 anos.

Tabela 5: Categorias de classificação da probabilidade

A tabela 6 classificação do impacto também é resultado da adaptação da tabela em vigor na EIB, no âmbito da certificação ISO 9001, essa tabela enumera os níveis existentes e identifica as consequências para a EIB que podem estar ou não associadas com Segurança da Informação. No entanto, os itens a verde estão exclusivamente relacionados com a Segurança da Informação.

1 Devido à natureza das ocorrências, os intervalos de tempo apresentam algumas diferenças.

Impacto	Descrição
Desastroso (**5**)	O risco poderá representar pelo menos uma das seguintes consequências para a Organização: • Incumprimento legal que pode afetar a existência da Organização; • Perda irreversível de imagem/reputação; • Custos muito elevados para a resolução da situação, relacionados com os produtos e serviços prestados (> 5% da faturação anual estimada); • Perda significativa de receita (> 5% da receita anual estimada); • Recolha de produtos não conformes, de forma irreversível; • Paralisação de operações, atividades, programas e processos da EIB, que causam impactos irreversíveis nos objetivos;
Elevado (**4**)	O risco poderá representar pelo menos uma das seguintes consequências para a Organização: • Incumprimento legal que não afeta a existência da Organização; • Perda de imagem / reputação, reversível em menos de 6 meses; • Custos elevados para a resolução da situação, relacionados com os produtos e serviços prestados (1 a 5% da faturação anual estimada); • Perda de receita (1 a 5% da receita anual estimada); • Recolha de produtos não conformes, que apenas poderão voltar ao mercado após reprocessamento; • Perda irreversível de 1 Cliente ou perda de mais do que 1 Cliente, que poderá ser reversível; • Interrupção de operações, atividades, programas ou processos da EIB, que causam impactos de reversão muito difícil nos objetivos;

Contínua na próxima página...

Impacto	Descrição
Médio (**3**)	O risco poderá representar pelo menos uma das seguintes consequências para a Organização: • Perda de imagem / reputação, reversível em menos de 3 meses; • Custos para resolução da situação, relacionados com os produtos e serviços prestados, de 0,5 a 1% da faturação anual estimada; • Perda de receita, de 0,5 a 1% da receita anual estimada; • Recolha de produtos não conformes, que poderão voltar ao mercado sem reprocessamento (ex: apenas após reembalamento); • Perda de um Cliente, que poderá ser reversível; • Interrupção de operações ou atividades da organização, programas ou processos, que causam impactos significativos nos objetivos, porém recuperáveis;
Baixo (**2**)	O risco poderá representar pelo menos uma das seguintes consequências para a Organização: • Custos para resolução da situação (relacionados com os produtos e serviços prestados), de 0,1 a 0,5% da faturação anual estimada; • Perda de receita, de 0,1 a 0,5% da receita anual estimada; • Produtos não conformes, que ainda não estão no mercado; • Reclamação de Cliente (s), sem perda do (s) mesmo (s); • Degradação de operações, atividades, programas ou processos da organização, causando impactos pequenos nos objetivos da EIB.

Contínua na próxima página...

Impacto	Descrição
Mínimo (**1**)	O risco poderá representar pelo menos uma das seguintes consequências para a Organização: • Custos para resolução da situação (relacionados com os produtos e serviços prestados), até 0,1% da faturação anual estimada; • Perda de receita, até 0,1% da receita anual estimada; • Degradação de operações, atividades, programas ou processos da organização, causando impactos mínimos nos objetivos da EIB.

Tabela 6: Categorias de classificação do Impacto

5.4.2 *Metodologia de análise dos riscos*

O Centro Nacional de Cibersegurança define no seu guia de gestão dos riscos que a análise de riscos pode ter uma abordagem de forma analítica com carácter qualitativo, quantitativo ou ambos.

- **Análise qualitativa**
  Para identificar a gravidade dos possíveis impactos e a probabilidade de ocorrência, utiliza-se uma escala de atributos qualitativos. Essa escala classifica os impactos em categorias que podem ir desde baixo, significativo, elevado, extremo, entre outros. No entanto, é importante destacar que essa abordagem apresenta uma desvantagem, a subjetividade da escala utilizada. Portanto, é necessário que as análises qualitativas se baseiem em dados e informações factuais para garantir a precisão dos resultados.
- **Análise quantitativa**
  Envolve a utilização de uma escala numérica para avaliar os impactos e probabilidades associados, requer a utilização de várias fontes de dados para garantir a qualidade da análise. A precisão e integridade dos valores numéricos, bem como a validade dos modelos utilizados, são fundamentais para obter resultados confiáveis. A principal vantagem da análise quantitativa é a sua relação direta com os objetivos e preocupações de segurança da informação da organização, uma vez que

utiliza dados históricos de incidentes. No entanto, essa abordagem pode apresentar desvantagens se não houver dados factuais e auditáveis disponíveis, o que pode levar a uma ilusão de precisão e eficácia no processo de avaliação de risco.

A EIB utiliza uma análise de gestão de riscos **qualitativa**. Esta abordagem permite uma maior flexibilidade e adaptabilidade, sendo especialmente útil em ambientes complexos e em constante mudança, além de facilitar a comunicação e o comprometimento das partes interessadas, promovendo uma compreensão comum dos riscos.

5.4.3 *Matriz de risco*

Através da fórmula:

$$\textbf{Risco} = \textbf{Probabilidade (P) x Impacto (I)}$$

Resulta a tabela 7 matriz de riscos que permite caracterizar os diferentes níveis de criticidade dos eventos identificados na Segurança da informação.

A matriz de riscos é composta por várias categorias ou níveis de criticidade, atribuídos com base nos valores resultantes da multiplicação da probabilidade e do impacto. Essas categorias são definidas numa escala **qualitativa**, permitindo uma avaliação mais subjetiva dos riscos. Esta matriz permite à EIB identificar e classificar os riscos de forma clara e consistente, facilitando a priorização das ações e recursos na mitigação dos riscos mais críticos.

		Probabilidade				
		Rara	Improvável	Possível	Provável	Frequente
Impacto	Mínimo	1	2	3	4	5
	Baixo	2	4	6	8	10
	Médio	3	6	9	12	15
	Elevado	4	8	12	16	20
	Desastroso	5	10	15	20	25

Tabela 7: Matriz de riscos

5.4.3.1 *Níveis de criticidade*

Cada categoria ou nível de criticidade possui uma descrição que indica o grau de severidade do risco associado como pode ser visto na tabela 8.

Criticidade	**Níveis**
Baixa	Intervalo de [1 - 4]
Significativa	Intervalo de [5 - 9]
Elevada	Intervalo de [10 - 15]
Extrema	Intervalo de [16 - 20]
Inaceitável	Cisne Negro (25)

Tabela 8: Níveis de criticidade

Da tabela 8 níveis de criticidade resultam 5 níveis, um dos quais o Centro Nacional de Cibersegurança (CNCS) no seu guia de gestão dos riscos identifica como o "Cisne Negro"que são acontecimentos altamente improváveis de acontecer, mas que têm de ser considerados numa análise de riscos.

5.4.4 *Riscos a tratar*

A EIB define os riscos a serem tratados com base numa análise cuidadosa, tendo em conta os seus ativos, processos e objetivos estratégicos. Os riscos identificados são aqueles que representam uma potencial ameaça à segurança da informação e que podem ter um impacto negativo na confidencialidade, integridade e disponibilidade dos ativos da organização.

A definição dos riscos a serem tratados é feita através do processo estruturado, que envolve a identificação, avaliação e classificação dos riscos conforme a fórmula:

Risco = Probabilidade x Impacto

Os riscos podem estar relacionados com diversas áreas, tais como:

1. **Riscos tecnológicos**
   Riscos relacionados com a infraestrutura de TI, sistemas de informação, redes, dispositivos, vulnerabilidades de segurança, etc.
2. **Riscos operacionais**
   Riscos relacionados com processos internos da EIB, procedimentos de segurança, gestão de incidentes, gestão de alterações, entre outros.
3. **Riscos organizacionais**
   Riscos relacionados com a governança, estratégia, políticas, recursos humanos, conformidade legal e regulatória, entre outros.
4. **Riscos físicos**
   Riscos relacionados com segurança física, controlo de acesso, proteção de instalações e equipamentos, etc.
5. **Riscos humanos**
   Riscos relacionados com ações e comportamentos dos colaboradores, formação e consciencialização em segurança da informação, gestão de privilégios de acesso, entre outros.

Ao identificar e definir os riscos a serem tratados, a EIB poderá implementar medidas de controlo adequadas, tais como políticas, procedimentos (Capitulo 4.9) e ações de formação, visando reduzir a probabilidade de ocorrência, bem como minimizar o impacto dos riscos identificados.

É fundamental que a definição dos riscos esteja alinhada com os objetivos estratégicos da EIB e com os requisitos estabelecidos na norma ISO/IEC 27001, assim como leve em consideração as melhores práticas de segurança da informação, normas e regulamentações aplicáveis.

5.4.5 *Aceitar o risco*

Como mencionado anteriormente na secção 5.4.1, a EIB definiu um critério de risco **superior a 9** como limite para ações de tratamento de risco, o que significa que todos

os ativos de informação que apresentem um nível de risco abaixo desse limite serão considerados aceitáveis e não serão tomadas ações adicionais para mitigar esses riscos.

A abordagem adotada pela EIB permite uma concentração de esforços e recursos nos riscos mais relevantes e impactantes para a segurança da informação. Estabelecer um limite de risco aceitável, permite à EIB priorizar a implementação de medidas de segurança e tratamento de riscos que apresentam uma maior probabilidade de ocorrência e um impacto mais significativo.

Ao aceitar os riscos que se encontram abaixo do limite estabelecido, a EIB consegue alocar recursos de forma mais eficiente, direcionando-os para mitigar os riscos mais críticos. Desta forma assegura que os recursos sejam direcionados para as áreas onde são mais necessários, garantindo a segurança dos ativos de informação e a continuidade do negócio.

5.4.6 *Transferência de riscos*

A transferência de riscos é uma prática recomendada pela ISO/IEC 27001, que encoraja as organizações a considerarem opções de transferência de riscos como parte da sua estratégia de gestão de riscos. No caso da EIB, seguindo esta abordagem, procura-se identificar os riscos que podem ser mitigados por meio de contratos de seguro ou acordos contratuais com fornecedores.

Ao transferir os riscos para terceiros, a EIB reduz a sua exposição aos potenciais impactos negativos desses riscos, transferindo a responsabilidade para entidades especializadas. Desta forma permite que a organização concentre os seus recursos internos em áreas de maior prioridade e especialização, enquanto aproveita o conhecimento e as capacidades dos parceiros externos.

A transferência de riscos também pode ajudar a EIB a encontrar um equilíbrio entre a mitigação interna e a transferência de riscos para terceiros, permitindo uma distribuição eficiente de recursos, com base na avaliação de riscos e nas capacidades internas da organização, ao mesmo tempo que pode reduzir os custos e a complexidade associados à gestão de riscos.

5.5 CONTROLOS DE SEGURANÇA

A ISO/IEC 27005 define controlos de segurança da informação como medidas técnicas, organizacionais e de gestão para mitigar os riscos de segurança e garantir a confidencialidade, integridade e disponibilidade das informações.

A ISO/IEC 27005 fornece uma estrutura para a seleção e implementação de controlos de segurança com base na avaliação de riscos. Os controlos são agrupados em categorias e são aplicados conforme as necessidades e prioridades da organização. Alguns exemplos de categorias de controlos de segurança incluem:

- Controlos preventivos
  São projetados para impedir que um risco ocorra, por exemplo, um firewall é um controlo preventivo, pois é projetado para impedir o acesso não autorizado a uma rede.
- Controlos de deteção
  Projetados para detetar um risco que já ocorreu, por exemplo, um sistema de deteção de intrusão, projetado para detetar atividades suspeitas na rede.
- Controlos de resposta
  Idealizados para responder a um risco que já ocorreu, por exemplo, um plano de resposta a incidentes é projetado para guiar uma organização na resposta a um incidente de segurança.
- Controlos de recuperação
  Projetados para recuperar de um risco que já ocorreu, por exemplo, uma cópia de segurança de dados é um controlo de recuperação, projetado para permitir que uma organização restaure dados em caso de perda ou corrupção.

Existem diversas formas de controlo que podem ser aplicadas, tais como: processos; políticas; procedimentos; dispositivos; e outras ações. No entanto, é importante ressaltar que nem sempre esses controlos exercem o efeito de modificação pretendido ou assumido, podendo haver variações nos resultados (Centro Nacional de Cibersegurança, 2023).

A aplicação dos controlos de segurança é um processo contínuo, sujeito a revisões e atualizações regulares, à medida que novas ameaças e riscos surgem. A EIB deve realizar

monitorização e revisões periódicas para garantir a eficácia dos controlos implementados e fazer ajustes conforme necessário.

5.6 MATRIZ DE RISCOS E OPORTUNIDADES

Uma matriz de riscos e oportunidades no desenvolvimento de um SGSI é uma ferramenta que permite identificar, avaliar e classificar os diferentes riscos e oportunidades relacionados com a segurança da informação. Essa matriz utiliza critérios como impacto e probabilidade para determinar a gravidade e a urgência de cada risco ou oportunidade, auxiliando na análise e na priorização das ações necessárias para tratar os elementos identificados. A matriz de riscos e oportunidades facilita a organização, a comunicação e a tomada de decisões, proporcionando uma gestão mais eficaz e direcionada.

A matriz de riscos e oportunidades pode ser enquadrada na **cláusula 6.1** da ISO/IEC 27001 e é a **etapa 7 da fase de diagnóstico** do roadmap da Integrity.

Segue-se a imagem 28 com um excerto de uma matriz de riscos e oportunidades elaborada na EIB, que incorpora os princípios e conceitos discutidos nas secções anteriores.

MATRIZ DE RISCOS E OPORTUNIDADES

ACTUALIZADO EM: 27/06/2023

ATIVOS	VUNERABILIDADE	AMEAÇAS	Acções / Actividades de Controlo já implementadas	RISCO						Necessidade de novas acções / controlos	
				Prob	Tipo	Impacto			Valor		
						C	I	D		(S/N)	N.º Acção
SERVIDORES INTEL HW.0001 HW.0002 HW.0003 HW.0004 HW.0005 HW.0006	Suscetibilidade a falhas de energia	Falha de energia	- Servidor ligado a UPS	2	Tecnologicos	2	3	4	**6**	N	-
	Suscetibilidade a avarias	Avaria do equipamento	- Swaper (discos, fontes de alimentação, processadr, memória, placa de rede).	2	Tecnologicos	4	3	4	**7**	N	-
	Uso de suportes físicos de armazenamento	Falha dos dispositivos de armazenamento	- Raid 1 : 2 discos - Raid 5 : 6 discos (3 + 3) - Raid 6 : 6 discos (5 + 1) + 1 Spare	2	Tecnologicos	2	3	5	**6**	N	-
	Incorreta parametrização do(s) servidores	Incidentes de segurança - disponibilidade / integridade	- Atualizações automáticas - Simulacros	3	Tecnologicos	1	2	3	**6**	N	-
	Permissões de acesso inadequadas	Acesso lógico não autorizado	- Firewall Windows	2	Tecnologicos	5	4	3	**8**	N	-
	Uso de software não autorizado ou sem licenciamento adequado	Ataques maliciosos externos	- Acesso limitado à instalação de software no servidor	1	Fisicos	4	4	4	**4**	N	-
		Incumprimento legal	- Acesso limitado à instalação de software no servidor	1	Tecnologicos	2	2	2	**2**	N	-
	Operação fixa nas instalações da empresa	Acesso físico não autorizado	- instalações com alarme - Chave pessoal de acesso ao escritório - Sala de servidores com acesso restrito - Bastidor do servidor fechado (com chave)	1	Humanos	5	5	5	**5**	N	-
		Incêndio / catástrofes naturais	- Cópia de segurança integral no exterior das instalações - semanal; - cópia de segurança (Cloud) - diário (novos dados) - Existência de extinção automatica; - Não armazenamento de materiais na sala do servidor - Sistema de Detecção de Incendio na sala do servidor;	1	Fisicos	1	4	4	**3**	N	-
		Roubo	- instalações com alarme - Chave pessoal de acesso ao escritório - Sala de servidor com acesso restrito - Bastidor do servidor fechado (com chave) - Cópia de segurança integral no exterior das instalações - Semanal; - cópia de segurança (Cloud) - diário (novos dados) - Encriptação de dados	1	Fisicos	2	4	4	**3**	N	-
NAS RED.0050/51	Utilização	Avaria	- Idade média do parque informático; - Monitorização	2	Tecnologicos	1	3	4	**5**	N	-
UPS'S HW.0040-49	Sobre - Utilização	Redução de disponibilidade	Testes de carga - simulacro	2	Operacionais	1	1	2	**3**	N	-
	Utilização	Avaria / Redução disponibilidade	Testes de carga - simulacro	2	Operacionais	1	1	2	**3**	N	-
Rede - Comunicações RED.0000	Utilização - acesso à internet	"avaria" - quebras de redes	- 2 Fornecedores (NOS / VODAFONE) - existência de pen de acessp à internet	3	Operacionais	1	1	5	**7**	N	-
Router'S RED.0001/RED. 0002	Utilização	Avaria	- Idade média do parque informático; - Monitorização	2	Operacionais	1	1	3	**3**	N	-

Figura 28: Excerto de Matriz de Riscos e Oportunidades da EIB

5.7 RELATÓRIO DE ANÁLISE DE RISCO DO SGSI

Um relatório de análise de riscos num SGSI deve conter informações relevantes sobre a identificação, avaliação e tratamento dos riscos relacionados com a segurança da informação na organização é um entregável da **etapa 7 da fase de diagnóstico** do roadmap da Integrity. Segue-se uma estrutura básica como exemplo:

1. Introdução
    - Breve descrição do objetivo do relatório e contexto da análise de riscos;
    - Informações sobre a metodologia utilizada na análise.
2. Âmbito da análise de riscos
   Descrição do âmbito da análise, incluindo os ativos de informação considerados, os processos envolvidos e as áreas da organização abrangidas.
3. Identificação dos riscos
    - Lista dos riscos identificados durante a análise, com as respetivas descrições e fontes de ameaça;
    - Categorização dos riscos conforme os critérios estabelecidos.
4. Avaliação dos riscos
    - Avaliação dos riscos identificados com base em critérios de impacto e probabilidade;
    - Atribuição de níveis de risco a cada um dos riscos avaliados.
5. Tratamento dos riscos
    - Descrição das estratégias e medidas de tratamento propostas para tratamento dos riscos identificados;
    - Priorização das ações de tratamento com base nos níveis de risco e recursos disponíveis.
6. Plano de ação
    - Descrição das ações a serem implementadas para mitigar ou eliminar os riscos;

- Definição de responsáveis, prazos e recursos necessários para a implementação das ações.

7. Considerações finais
   - Conclusões gerais da análise de riscos.
   - Recomendações para a melhoria contínua da segurança da informação na organização.
8. Anexos (opcional)
   Documentos de apoio, como tabelas, logs de aplicações ou registos utilizados durante a análise.

É importante que o relatório seja claro, objetivo e baseado em informações precisas e atualizadas, deve ser revisto e aprovado pelas partes interessadas antes de ser divulgado e utilizado para orientar as ações de segurança da informação.

5.8 PLANO DE TRATAMENTO DE RISCOS

Durante a fase de Tratamento dos Riscos, são identificados, formalizados e implementados um ou mais planos de ação. Estes planos visam controlar e/ou mitigar as causas dos riscos identificados na fase de levantamento e fazem parte da **etapa 8 da fase de diagnóstico** do roadmap da Integrity.

No contexto da implementação dos planos de ação e ações de tratamento de riscos, é necessário designar um responsável e definir uma data para a sua implementação. O objetivo é que, ao concluírem os planos de ação, ocorra uma redução do nível de risco associado (Centro Nacional de Cibersegurança, 2023).

Os possíveis tratamentos de riscos estão descritos na seguinte lista:

1. **Aceitar**
   Reconhecer o risco e decidir não tomar nenhuma ação específica para o tratar, assumindo as possíveis consequências. No caso da EIB está assumido na secção 5.4.5 que serão aceites todos os riscos que apresentem um valor calculado de risco inferior a dez.

2. **Transferir**

   Transferir total ou parcialmente o risco para terceiros, como seguradoras, fornecedores ou parceiros de negócios, por meio de contratos ou acordos.

3. **Mitigar**

   Implementar medidas para reduzir a probabilidade de ocorrência do risco ou minimizar o seu impacto caso ocorra, pode envolver a implementação de controlos de segurança adicionais, formações, revisão de processos ou atualização de tecnologias.

4. **Evitar**

   Tomar ações para evitar completamente o risco, como interromper atividades específicas, remover ou substituir ativos vulneráveis, ou cancelar projetos que apresentem um elevado grau de risco.

A seguir apresenta-se a tabela 9 do tratamento de riscos para cada nível de riscos da EIB:

Valor Risco	**Intervalo**	**Tratamento recomendado**
Baixo	[1,4]	Aceitar
Significativo	[5,9]	**Aceitar**
Elevado	[10,15]	Mitigar/Transferir
Extremo	[16,20]	Mitigar/Transferir
Inaceitável	[25]	Evitar

Tabela 9: Tratamento dos riscos EIB

O departamento encarregado da análise, avaliação e tratamento dos riscos identificados tem a responsabilidade adicional de avaliar e elaborar os planos de tratamento dos riscos, seguindo o processo ilustrado na Figura 29.

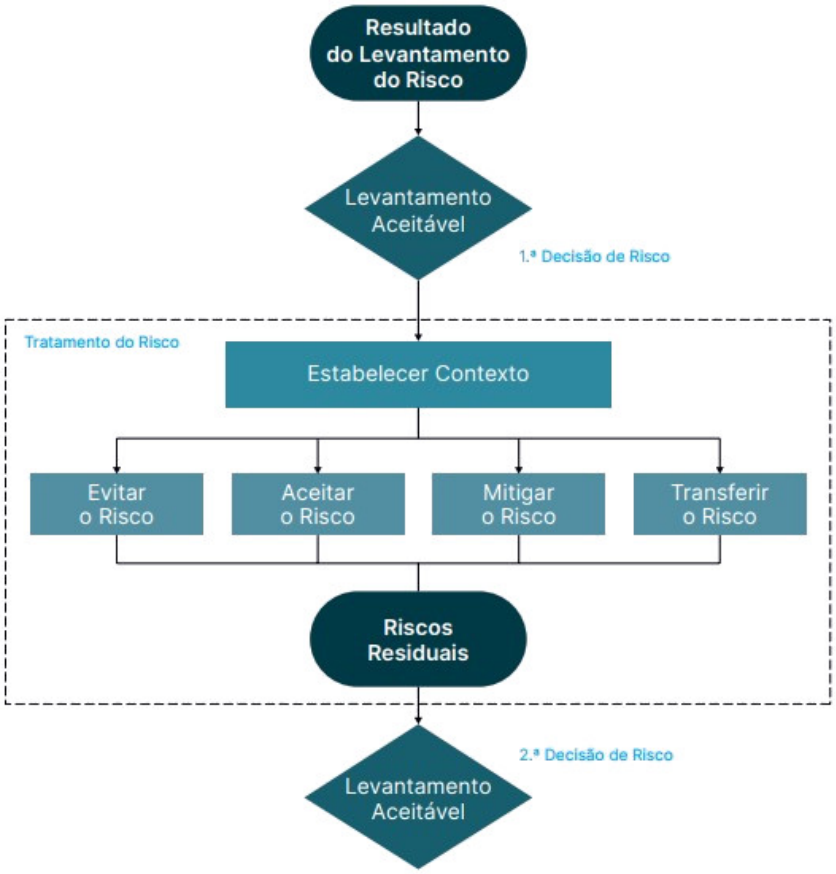


Figura 29: Tratamento dos Riscos ISO/IEC 27005 (Centro Nacional de Cibersegurança, 2023)

Os planos de tratamento dos riscos visam documentar as opções tomadas, como serão implementadas e a sequência em que serão executadas e devem ser registados numa ferramenta ou sistema, para permitir o acompanhamento e a gestão eficaz. Estes planos devem incluir informações detalhadas sobre o processo de escolha e implementação dos tratamentos, tais como (Centro Nacional de Cibersegurança, 2023):

- Razão das escolhas e os benefícios que se pretende alcançar através delas;
- Definição das etapas e atividades necessárias para a implementação de cada tratamento;
- Atribuição de responsabilidades para a execução das atividades;
- Estabelecimento de prazos e cronograma para a implementação dos tratamentos;

- Identificação dos recursos necessários, como pessoal, tecnologia ou orçamento;
- Definição dos critérios para avaliar a eficácia dos tratamentos implementados;
- Monitorização contínua dos tratamentos e revisão periódica para assegurar a sua eficácia e efetuar ajustes, se necessário.

A tabela 10 a seguir apresenta um exemplo de processo a ser implementado na fase de "Tratamento de Riscos", onde o ciclo de avaliação e implementação de tratamento de riscos é repetido após a sua conclusão.

Inputs	**Atividades**	**Outputs**
Riscos analisados	• Desenvolvimento de opções de tratamento dos riscos; • Planificação de tratamentos dos riscos; • Seleção de opções de tratamento; • Implementação de tratamentos dos riscos; • Análise da eficiência e eficácia dos tratamentos realizados; • Monitorização e revisão dos controlos implementados conforme os planos de tratamento dos riscos.	• Opções de tratamento; • Planos de tratamento dos riscos.

Tabela 10: Tratamento dos riscos (Centro Nacional de Cibersegurança, 2023)

5.9 COMUNICAÇÃO E CONSULTA DOS RISCOS

A Comunicação e Consulta dos Riscos é uma atividade contínua que visa alcançar o consenso sobre a gestão dos riscos de segurança da informação e cibersegurança, promovendo a troca de informações entre os responsáveis e as partes interessadas. É importante garantir o alinhamento das perceções de risco e benefícios entre as partes interessadas, além de promover a consciencialização sobre a importância da gestão de riscos em toda a organização.

A coordenação e discussão dos riscos podem ser facilitadas por um grupo de trabalho específico, que prioriza e trata adequadamente os riscos, incluindo a sua aceitação. É

recomendada a realização periódica de revisões de riscos e verificações do estado dos planos de tratamento, com apresentações e análises dos resultados para a gestão de topo, a fim de subsidiar tomadas de decisão e demonstrar responsabilidade sobre os riscos.

É de grande valor estabelecer uma cultura de gestão de riscos na organização e comunicar a estratégia e/ou política de gestão de riscos. A cooperação com departamentos de comunicação e relações externas também é fundamental, especialmente em situações de crise ou na preparação de informações em resposta a incidentes específicos.

Recomenda-se que a organização estabeleça um plano e práticas de comunicação e consulta de riscos, assegurando que todas as decisões e modificações sejam comunicadas através dos canais estabelecidos. A informação partilhada deve ser adequada para atingir os objetivos do processo de gestão de riscos e da organização, e deve ser derivada das decisões tomadas no processo de gestão de riscos. As partes externas devem ser informadas sobre as decisões relevantes do processo de gestão de riscos, quando aplicável, e os canais de comunicação devem ser utilizados para fortalecer a confiança e a consciencialização das partes externas relativamente aos riscos e decisões da organização (Centro Nacional de Cibersegurança, 2023).

5.10 MONITORIZAÇÃO E REVISÃO DOS RISCOS

A organização deve realizar uma monitorização contínua do ecossistema de risco de segurança da informação, isto porque os riscos não são estáticos, e as ameaças, vulnerabilidades, probabilidades e consequências estão sempre em mudança. Qualquer alteração significativa no contexto interno ou externo da organização pode afetar a perceção do risco. A monitorização e revisão dos riscos são realizadas de forma contínua ao longo do processo de gestão de riscos.

A monitorização e análise crítica dos riscos têm vários objetivos, incluindo verificar a eficácia dos controlos implementados, obter informações para melhorar o processo de avaliação de riscos, analisar eventos e incidentes para aprender com eles minimizando ocorrências futuras, identificar mudanças que podem afetar a classificação e tratamento dos riscos, e identificar riscos emergentes.

Recomenda-se que os resultados de todas as fases do processo de gestão de riscos sejam registados para estudo e aperfeiçoamento contínuo, além de auxiliar na análise de desempenho dos procedimentos e ferramentas implementados.

A monitorização contínua é fundamental para garantir que o contexto, os resultados da avaliação e tratamento dos riscos, bem como os planos de gestão, permaneçam relevantes e adequados às circunstâncias. A organização deve monitorizar continuamente novos ativos, alterações na criticidade dos ativos, novas ameaças, possíveis vulnerabilidades, aumento do impacto dos riscos e incidentes de segurança da informação, tanto os ocorridos quanto os potenciais (Centro Nacional de Cibersegurança, 2023).

5.11 GESTÃO DE INCIDENTES DE SI

O procedimento de registo e gestão de incidentes de segurança da informação **etapa 14 da fase de operação** do roadmap da Integrity é fundamental, pois assume uma resposta eficiente e eficaz a eventos que possam afetar a integridade, confidencialidade e disponibilidade dos ativos de informação da organização. A EIB implementou no âmbito deste projeto a aplicação "GLPI"como uma ferramenta centralizada para fazer o registo e o acompanhamento dos incidentes de segurança da informação.

1. **Registo de Incidentes**
   O registo de incidentes de segurança da informação pode ser realizado através de uma das seguintes vias:

   - Registo via Aplicação "GLPI"
     Todos os colaboradores da EIB têm acesso à aplicação "GLPI"via navegador de internet para reportar incidentes de segurança da informação. Ao detetar um incidente, o colaborador deve registá-lo na aplicação, fornecendo informações detalhadas sobre a natureza do incidente, data e hora de ocorrência, possíveis impactos e quaisquer outros detalhes relevantes. O procedimento de registo está disponível em C.2

   - Registo por Formulário Específico
     Em caso de falência dos sistemas informáticos ou indisponibilidade da aplicação "GLPI", existe um formulário específico que pode ser preenchido manualmente

e entregue ao departamento de SI. Esse formulário permitirá ao colaborador reportar o incidente mesmo quando a aplicação não estiver disponível.

- Registo por Chamada Telefónica ou Email
  Em situações de emergência ou incidentes graves, os colaboradores têm a opção de reportar o incidente por meio de uma chamada telefónica direta para o departamento de SI ou enviando um email para um endereço específico "ReportSI@eib.pt"designado para esse fim.

2. **Tratamento e Acompanhamento do Incidente**
   Uma vez registado, o incidente este é encaminhado para a equipa de resposta a incidentes da EIB para avaliação e tratamento adequado. A equipa tomará as medidas necessárias para conter, investigar e mitigar o incidente, garantindo a continuidade das operações e minimizando os possíveis impactos negativos.

3. **Notificações das Partes Interessadas**
   A equipa de resposta a incidentes garantirá a notificação apropriada às partes interessadas internas e externas, conforme necessário. Podendo incluir a comunicação à direção, aos colaboradores afetados, aos clientes e fornecedores relevantes, bem como às autoridades reguladoras, quando aplicável.

4. **Responsáveis pelo Tratamento e Acompanhamento**
   A equipa de resposta a incidentes será constituída por um membro com responsabilidades específicas para o tratamento e acompanhamento de cada incidente, esse membro será responsável por assegurar que o incidente seja resolvido adequadamente e que todas as ações necessárias sejam tomadas para evitar recorrências.

A B.13 política e o C.2 procedimento de registo e gestão de incidentes de segurança da informação da EIB visam garantir uma resposta rápida e eficiente a qualquer evento que possa afetar a segurança da informação. A implementação de uma aplicação dedicada, bem como a disponibilidade de alternativas de registo em casos de falência dos sistemas informáticos, reforçam a abordagem proativa e resiliente da EIB na proteção dos ativos de informação.

5.12 CASO USO REAL - SEGREGAÇÃO DA REDE ZEPPELIN

Nesta secção, será apresentado um caso de uso real de um ativo que possui um risco classificado como superior a nove como se pode verificar na tabela 30 de riscos e oportunidades. De acordo com o definido na secção 5.4.1, este risco apresenta um grau de criticidade "**Elevada**" e será submetido a um processo de tratamento para mitigar o perigo que representa para a EIB.

MATRIZ DE RISCOS E OPORTUNIDADES

ACTUALIZADO EM: 27/06/2023

ATIVOS	VUNERABILIDADE	AMEAÇAS	Acções / Actividades de Controlo já implementadas	RISCO						Necessidade de novas acções / controlos	
				Prob	Tipo	Impacto			Valor	(S/N)	N.º Acção
						C	I	D			
Rede Zeppelin RED.0010	Utilização	Acesso Indevido	- Implementar segregação de redes - Substituição de Switchs - Identificação de cablagem	3	Operacionais	4	3	5	**12**	S	**INC.00001**
	Hardware Legacy	Avaria	- Substituição de equipamentos (sempre que possivel)	2	Operacionais	3	3	5	**7**	N	

Figura 30: Ativo com risco superior a nove

5.12.1 *Estabelecer o Contexto*

O tratamento do risco identificado na rede industrial ICS Zeppelin, que é o coração produtivo da EIB, é de extrema relevância para garantir a segurança e continuidade das operações da organização, a rede industrial Zeppelin representa um ativo crítico para a EIB, pois está diretamente relacionada com a produção e a eficiência dos processos fabris.

Este ativo ainda apresenta alguns riscos, nomeadamente o uso de hardware e software muito antigos, os quais não podem ser atualizados devido ao elevado risco de disrupção das operações na secção da Mistura e ao elevado custo de investimento que representa um projeto de atualização. No entanto, estes riscos devem ser considerados para o futuro, com a perspetiva de garantir a continuidade do negócio.

Pretende-se isolar completamente esta rede das demais existentes na EIB, implementando uma abordagem "**Zero Trust Network**", devido à dificuldade em atualizar os sistemas operativos e instalar endpoints atuais, espera-se que esta medida torne a rede atual mais resiliente a ameaças, principalmente a ataques de "Ransomware", que possam surgir a partir de redes internas.

5.12.1.1 *Âmbito*

O tratamento deste risco abrangerá toda a rede industrial da secção da Mistura, incluindo switches, computadores, placas de pesagem (MB's) e autómatos, serão tomadas medidas específicas para garantir a segurança e a mitigação de potenciais impactos associados a estes ativos.

5.12.1.2 *Responsabilidades*

O departamento de TI tem a responsabilidade de planear e implementar ações de mitigação, contando com a colaboração do departamento de manutenção e a aprovação dos departamentos de produção e da gestão de topo.

5.12.2 *Plano de Tratamento*

Para mitigar o risco identificado na rede industrial Zeppelin, será apresentado um plano de ação abrangendo várias fases, no qual serão identificados os responsáveis pelas ações a serem executadas e implementada uma abordagem de "Zero Trust Network".

5.12.2.1 *Objetivo*

Mediante a implementação deste plano de ações, o objetivo é mitigar o risco de acesso não autorizado à rede industrial Zeppelin, tornando-a mais resistente e menos exposta e vulnerável a agentes maliciosos.

5.12.2.2 *Recursos*

Para implementar este plano, será necessário adquirir dois switchs Cisco ou HPE de layer 3, cada um com 48 portas Gigabit e 4 portas SFP. Além disso, será necessário solicitar a colaboração de um eletricista para identificar as cablagens que ainda não estão devidamente identificadas e instalar os switchs nos respetivos bastidores.

5.12.2.3 *Cronograma*

Esta ação deve ser implementada na semana programada de paragem para manutenção de 7 a 11 de agosto.

5.12.2.4 *Etapas*

A seguir estão enumeradas as etapas necessárias para a execução deste plano:

1. Configuração dos switches - Responsável (RP) DTI;
    - Atribuição dos endereços IP de gestão;
    - Configuração das VLAN;
    - Configuração dos Trunks;
    - Configuração das ACL;
    - Configuração de inter-VLAN routing;
    - Configuração de rotas alternativas;
    - Backup das configurações.
2. Instalação física nos bastidores - RP Eletricista;
3. Identificação de cablagem e respetivas portas nos switch's - RP Eletricista;
4. Testes - RP DTI;
5. Remoção dos switchs antigos - RP Eletricista.

5.12.3 *Avaliação e Monitorização*

Para avaliar adequadamente a implementação dessa ação, é necessário realizar testes de acesso das várias redes existentes na EIB, garantindo assim que nenhuma delas tenha acesso à rede Zeppelin. Adicionalmente, é fundamental registar todos os pedidos de abertura de portas ou solicitações de acesso a sistemas de controlo, para possibilitar um controlo de acessos e uma monitorização das atividades na rede.

5.13 SÍNTESE

Em síntese, o capítulo de Gestão de Riscos assume especial importância para o Sistema de Gestão de Segurança da Informação (SGSI) da EIB. Neste capítulo, foram definidos os seguintes elementos:

- Definição e Caracterização de Ativos
  Identificaram-se ativos de informação da EIB, tendo em conta a sua importância e sensibilidade para a organização. Cada ativo foi valorizado com base em critérios como valor, criticidade e sensibilidade das informações.
- Metodologia de Avaliação de Risco
  Optou-se pela análise de risco qualitativa como a metodologia preferencial para avaliar os riscos associados aos ativos de informação da EIB. Esta abordagem utiliza escalas de atributos de qualificação para identificar a severidade dos potenciais impactos e a sua probabilidade de ocorrência.
- Matriz de Risco e Oportunidades
  Foi criada uma matriz de risco e oportunidades para mapear os riscos identificados em relação à sua probabilidade e impacto. Esta matriz auxilia na classificação dos riscos em diferentes níveis de criticidade, facilitando a priorização e o desenvolvimento de estratégias de tratamento adequadas.
- Plano de Tratamento de Riscos
  Com base nos resultados da análise de risco, elaborou-se um esboço do plano de tratamento de riscos.
- Relatório de Análise de Riscos
  Elaborou-se um esboço de relatório que documenta o processo de análise de riscos, incluindo a identificação dos ativos, avaliação e tratamento dos riscos e plano de ação.
- Gestão de Incidentes de Segurança da Informação
  Estabeleceu-se um procedimento para o registo e gestão de incidentes de segurança da informação na EIB. Este procedimento inclui a utilização da plataforma GLPI em my.eib.pt para registar e acompanhar os incidentes.

- Caso Uso
  Foi apresentado o tratamento de riscos de um caso de uso real, apresentando o Contexto, Âmbito, Responsabilidades, Plano de Tratamento e Avaliação.

O capítulo de Gestão de Riscos do SGSI da EIB foi desenvolvido em conformidade com a norma ISO/IEC 27005 e teve como base de suporte a documentação disponibilizada pelo Centro Nacional de Cibersegurança (CNSC), especificamente o "Guia para Gestão dos Riscos em Matérias de Segurança da Informação e Cibersegurança".

6

MONITORIZAÇÃO, AVALIAÇÃO, COMUNICAÇÃO E MELHORIA CONTÍNUA

Neste capítulo, será realizada uma breve abordagem à **cláusula 9 e 10** "Avaliação e Desempenho"e "Melhoria Contínua"da norma ISO/IEC 27001, que explora a monitorização e melhoria contínua do Sistema de Gestão de Segurança da Informação (SGSI), auditorias e revisão do SGSI. Serão também definidas métricas para avaliar o desempenho do SGSI e além disso, serão abordados os temas de formação, consciencialização e comunicação, incluindo um plano de simulacros.

Considerando que este projeto marca o início da implementação do SGSI na EIB, é natural que ainda não seja possível avaliar na totalidade o estado de implementação e execução do mesmo.

6.1 MONITORIZAÇÃO DO SGSI

A monitorização do SGSI é abordada na **cláusula 9.1** da norma ISO/IEC 27001, intitulada "Monitorização, análise crítica e avaliação" é também a **etapa 15 da fase de operação** do roadmap da Integrity. Esta cláusula estabelece os requisitos para que a organização acompanhe e avalie de forma sistemática o desempenho e a eficácia do seu SGSI.

Esta cláusula exige que a organização implemente processos para monitorizar, medir e avaliar regularmente o desempenho do SGSI. Deve incluir indicadores de desempenho, métricas e outros parâmetros relevantes para verificar a conformidade com os requisitos do SGSI.

A avaliação de conformidade é outro aspeto importante nesta cláusula, onde a organização deve avaliar regularmente se o SGSI está a ser operado conforme as políticas, procedimentos e controlos definidos.

Adicionalmente, a norma requer a manutenção de registos documentados das atividades de monitorização, análise crítica e avaliação do SGSI, esses registos são fundamentais para comprovar a conformidade do SGSI com a ISO/IEC 27001 e possibilitar uma análise posterior dos resultados obtidos.

6.2 MÉTRICAS E INDICADORES DE SI

As métricas e indicadores são um entregável da **etapa 15 da fase de operação** do roadmap da Integrity e essenciais para avaliar o desempenho do SGSI da EIB e identificar áreas que requerem melhorias ou ajustes para fortalecer a segurança da informação da organização. É importante adaptar as métricas e indicadores conforme os objetivos e requisitos específicos da EIB, bem como com as normas e regulamentos aplicáveis ao setor onde atua.

A definição de métricas de Segurança da Informação (SI) para o SGSI da EIB deve estar alinhado com os objetivos estratégicos da empresa e levar em consideração as características específicas do setor. Algumas métricas incluem:

1. Taxa de incidentes de segurança
   Número de incidentes de segurança reportados durante um período, como ataques cibernéticos, violações de dados ou tentativas de intrusão.
2. Tempo médio entre deteção e resposta:
   Tempo decorrido entre a deteção de um incidente de segurança e a sua resolução. Quanto menor for esse tempo, mais eficiente é a resposta da organização a incidentes.
3. Taxa de cumprimento de políticas e procedimentos
   Percentagem de colaboradores e utilizadores que cumprem as políticas e procedimentos estabelecidos de segurança da informação.
4. Percentagem de sistemas e dispositivos atualizados
   Indica a percentagem de sistemas, aplicações e dispositivos que estão atualizados com as últimas correções e atualizações de segurança.
5. Nível de consciencialização
   Mede a eficácia das ações de consciencialização em segurança da informação na or-

ganização, com base na participação e compreensão dos colaboradores relativamente às boas práticas de segurança.

6. Nível de conformidade com a ISO/IEC 27001
   Avalia o grau de conformidade do SGSI da EIB com os requisitos da norma ISO/IEC 27001.

7. Tempo médio de resposta a incidentes
   Mede o tempo médio que o departamento de SI leva para investigar, responder e mitigar um incidente de segurança da informação.

8. Taxa de sucesso em auditorias internas e externas
   Mede a eficácia do SGSI em passar em auditorias de segurança realizadas interna e externamente.

9. Nível de segurança da rede industrial (ICS):
   Avalia o nível de segurança das redes industriais que suportam os processos de produção e controlo da EIB.

10. Taxa de Conformidade com Normas e Regulamentos
    Mede o grau de conformidade da EIB com as normas e regulamentos de segurança da informação aplicáveis, como ISO/IEC 27001 e obrigações legais tais como o RGPD.

11. Taxa de utilização de ferramentas de monitorização e deteção de ameaças
    Mede o grau de adoção e eficácia das ferramentas de monitorização e deteção de ameaças utilizadas pela EIB.

6.3 COMUNICAÇÃO

No âmbito da comunicação **Clausula 7.4** da ISO/IEC 27001, a EIB deve assegurar uma comunicação eficaz relativamente à segurança da informação, envolvendo a definição de processos de comunicação claros e bem definidos, que permitam a transmissão de informações relevantes e oportunas a todas as partes interessadas.

Essa comunicação abrange desde a divulgação das políticas e procedimentos de segurança da informação para todos os colaboradores da organização, até a notificação

e relato de incidentes de segurança às autoridades competentes e partes interessadas externas. É fundamental garantir que todos os colaboradores estejam conscientes das responsabilidades subjacentes à segurança da informação e que saibam como agir em caso de incidentes ou violações.

Além disso, é importante que a EIB mantenha uma lista atualizada de contactos relevantes das partes interessadas e das autoridades competentes. Inicialmente, esta lista já existia nos sistemas de gestão da EIB, mas foi recentemente revista e atualizada para incluir novos contactos conforme o âmbito da segurança da informação. Esta lista inclui informações de contacto de pessoas-chave dentro e fora da organização, com funções na segurança da informação ou que precisem de ser notificadas em casos de incidentes.

Ter uma comunicação eficaz e uma lista de contactos atualizada são elementos muito importantes para garantir uma resposta rápida e adequada a eventos de segurança da informação, permitindo a coordenação entre todas as partes envolvidas e a mitigação eficiente de riscos.

6.4 REVISÃO DO SGSI

A **cláusula 9.3** da ISO/IEC 27001 dedicada à "Análise crítica pela gestão" e **etapa 16 da fase de operação** do roadmap da Integrity, representa um elemento valioso para o sucesso do SGSI na organização. Nessa fase, a gestão de topo da empresa deve realizar uma revisão periódica e aprofundada do desempenho do SGSI para garantir a eficácia, bem como a conformidade com os objetivos definidos e o alinhamento com as estratégias do negócio.

Durante a análise crítica, são avaliados aspetos como a eficácia dos controlos de segurança, a identificação de não conformidades e a tomada de ações corretivas quando necessário. São ainda considerados os resultados de análises de riscos, permitindo a identificação de novos riscos ou oportunidades relacionadas com a segurança da informação. Essa avaliação é determinante para assegurar que o SGSI esteja adequado à natureza e complexidade dos processos e informações da organização.

Através da análise crítica, a gestão de topo identifica oportunidades de melhoria no SGSI e define ações para alcançar melhores resultados, esta prática de melhoria

contínua enquadrada com o ciclo PDCA garante que o SGSI permanece atualizado, efetivo e conforme os requisitos do negócio, proporcionando um ambiente seguro para as informações e ativos da organização.

Registos de revisão do SGSI pela gestão de topo

Segundo o roadmap definido pela (Integrity, 2023) após a realização da revisão do SGSI a empresa deve analisar, rever e registar alguns pontos importantes para garantir a eficácia e a melhoria contínua do sistema. Alguns desses pontos a serem registados são:

- Desempenho do SGSI
  Avaliação global do SGSI relativamente aos objetivos e metas estabelecidos, tendo em conta a eficácia dos controlos implementados e o alcance das melhorias planeadas.
- Resultados de auditorias e avaliações
  Análise dos resultados de auditorias internas e externas, bem como outras avaliações de conformidade, para identificar eventuais não conformidades e oportunidades de melhoria.
- Níveis de risco
  Verificação dos níveis de risco identificados no SGSI e das ações tomadas para mitigar ou aceitar os riscos, garantindo a conformidade com a estratégia de gestão de riscos da organização.
- Ocorrência de incidentes
  Análise de incidentes de segurança da informação ocorridos desde a última revisão, incluindo as ações corretivas adotadas e as medidas para prevenir a recorrência.
- Implementação de ações corretivas
  Verificação do progresso na implementação das ações corretivas identificadas em revisões anteriores e da sua eficácia na resolução de não conformidades.
- Melhorias no SGSI
  Identificação de oportunidades para aperfeiçoar o SGSI, com base nas melhores práticas, novas tecnologias ou experiências adquiridas.

- Recursos e competências
  Verificar a disponibilidade de recursos, incluindo pessoal qualificado e treinado, para apoiar o funcionamento e execução do SGSI.
- Comunicação e consciencialização
  Avaliação do desempenho das atividades de comunicação e consciencialização em segurança da informação para todas a partes interessadas.
- Alinhamento com a estratégia do negócio
  Garantia de que o SGSI esteja alinhado com a estratégia geral da organização e os seus objetivos de negócio.

6.5 AUDITORIAS INTERNAS

Calder, 2009 refere que as auditorias são especificamente projetadas e planeadas para garantir que os controlos documentados na Declaração de Aplicabilidade (SoA) sejam eficazes e estejam a ser aplicados, para identificar não conformidades e oportunidades de melhoria. Estas estão representadas na **etapa 17 da fase de operação** do roadmap da Integrity.

O objetivo de **controlo A 18.2.2** (Conformidade com políticas e normas de segurança) trata especificamente com esta questão e exige revisões regulares e planeadas de conformidade, tanto ao nível dos processos como ao nível técnico "O **controlo A.18.2.3** trata dos requisitos de segurança para conformidade técnica".

O requisito de auditorias é descrito com mais profundidade na **cláusula 9.2** da ISO 27001, que estabelece dois aspetos importantes do processo:

- O programa de auditoria deve ser planeado, tendo em consideração o estado e a importância dos processos e áreas a serem auditados, bem como os resultados de auditorias anteriores.
- A gestão responsável pela área que está a ser auditada deve garantir que as ações são tomadas sem demora para eliminar as não conformidades detetadas e as suas causas.

A Norma é clara ao afirmar que a gestão a todos os níveis da organização tem um papel eficiente a desempenhar na implementação, manutenção e melhoria do SGSI. Isso deve ser considerado em descrições de funções de gestão e supervisão, contratos de emprego, formações, bem como em avaliações de desempenho (Calder, 2009).

As auditorias internas têm como objetivo avaliar a conformidade do SGSI com os requisitos da norma ISO/IEC 27001, bem como verificar a eficácia das medidas de segurança implementadas, essas auditorias são conduzidas por auditores internos com competências adequadas, estes devem ser independentes das áreas que estão a ser auditadas e adicionalmente devem manter registos das respetivas atividades de auditoria. As auditorias internas devem ser realizadas periodicamente, conforme um plano estabelecido pela gestão de topo e devem abranger todas as áreas relevantes do SGSI.

6.6 FORMAÇÃO E CONSCIENCIALIZAÇÃO

A **cláusula 7** da ISO/IEC 27001 inclui duas secções que tratam do tema da formação e consciencialização, sendo também a **etapa 12 da fase de operação** do roadmap da Integrity, a saber:

> **Cláusula 7.2 - Competência**
> A cláusula é dedicada ao tema da competência das pessoas que estão envolvidas na implementação do SGSI, esta cláusula realça a importância de garantir que estas pessoas possuem as competências necessárias para desempenhar tais funções e que, estão devidamente instruídas.
>
> A **formação** destes quadros pode ser realizada internamente ou por meio de cursos e certificações externas, a organização deve fornecer oportunidades de desenvolvimento contínuo para atualizar as competências dos indivíduos, conforme a evolução tecnológica e de negócio.
>
> **Cláusula 7.3 - Consciencialização**
> A cláusula foca a importância de criar uma cultura de segurança da informação consciente entre as partes interessadas, realçando que a **consciencialização** sobre a política de segurança da informação, objetivos do SGSI e importância da confor-

midade com os requisitos de segurança da informação, devem ser estabelecidos e mantidos.

Para cumprir com os requisitos, a organização deve implementar programas de consciencialização em SI que abordem as principais ameaças e riscos de segurança, bem como as medidas de proteção e boas práticas. Esses programas devem incluir formações, comunicações internas entre outras iniciativas garantindo que todos os colaboradores estejam cientes do papel que desempenham na segurança da informação e que compreendem as ações que devem tomar para proteger os ativos de informação da organização.

6.7 SIMULACROS E PLANO DE SIMULACROS

Os simulacros são atividades e práticas simuladas que testam a capacidade de resposta da organização a incidentes de segurança da informação. Estes verificam a eficácia dos controlos de segurança, simulando cenários de risco, permitindo melhorias nos procedimentos e treinos. Fortalecem a consciencialização e promovem uma cultura de segurança.

Segundo o Centro Nacional de Cibersegurança, no "Roteiro para Capacidades Mínimas de Cibersegurança" determina que os simulacros em cibersegurança devem ser realizados pelo menos uma vez por ano.

PLANO DE SIMULACROS DE SEGURANÇA DA INFORMAÇÃO NA EIB

Objetivo

O objetivo deste plano é estabelecer um programa de simulacros de segurança da informação na EIB com o propósito de testar e avaliar a eficácia das medidas de segurança implementadas, bem como a resposta da organização a incidentes de segurança da informação.

Âmbito

O plano de simulacros abrange todas as áreas da EIB que de alguma forma se relacionam com informações e sistemas críticos para o funcionamento da empresa.

Responsabilidades

O Departamento de Segurança de Informação (DSI) será responsável pela aprovação e revisão periódica do plano de simulacros e pela coordenação e execução dos simulacros. Todos os outros departamentos serão responsáveis por participar nos exercícios do simulacro e colaborar nas ações corretivas e preventivas.

Procedimentos

- Serão realizados pelo menos dois simulacros de segurança da informação por ano, abordando cenários diferentes, como ataques de ransomware, violação de dados, interrupção de serviços, entre outros.
- Antes de cada simulacro, será definido um cenário específico e um conjunto de objetivos a serem alcançados.
- As ações a serem tomadas estarão apenas disponíveis no responsável pelo DSI, para garantir a autenticidade do exercício.
- Após cada simulacro, será realizado um briefing com os participantes para discutir os resultados, lições aprendidas e identificar áreas de melhoria.
- Todas as conclusões e recomendações resultantes dos simulacros serão documentadas e apresentadas à gestão de topo para revisão e implementação de ações corretivas.

Conclusões

O plano de simulacros de segurança da informação visa aperfeiçoar a capacidade de resposta da EIB em situações de incidentes de segurança, identificar eventuais lacunas no sistema de gestão de segurança e fortalecer a consciencialização e a competência dos colaboradores em relação com proteção de ativos de informação da empresa.

Nota: A plataforma GLPI em my.eib.pt será utilizada para registar todas as informações pertinentes com os simulacros, incluindo os cenários, resultados e ações corretivas.

6.8 MELHORIA CONTINUA

A melhoria contínua **Clausula 10.2** da ISO/IEC 27001 é um aspeto importante a ter em consideração, mesmo após a implementação dos controlos padrão da norma ISO/IEC 27001 e a certificação por um organismo externo. Muitas organizações não se concentram em procurar melhorias adicionais após a certificação, assumindo que os controlos normais garantem a segurança das informações da empresa. No entanto, é fundamental manter o foco na verificação e na ação para assegurar a segurança da informação. Realizar verificações regulares nos controlos de segurança e nas políticas é essencial para identificar lacunas e, em seguida, atuar para implementar melhorias. Este processo é um ciclo contínuo e exige atenção constante para manter a segurança da informação atualizada (Chopra e Chaudhary, 2020).

A melhoria contínua é um princípio fundamental da norma ISO/IEC 27001 e está presente em todo o seu contexto. Neste sentido, a EIB deve adotar uma abordagem sistemática para identificar oportunidades de melhoria no seu SGSI e implementar ações corretivas e preventivas para fortalecer continuamente a segurança da informação.

A postura proativa relativamente à segurança da informação permitirá que a EIB esteja preparada para enfrentar desafios futuros e responder de forma resiliente a ameaças em constante evolução.

Para atingir o objetivo de melhoria contínua, a EIB pode seguir algumas práticas:

- Realizar análises críticas periódicas dos resultados das auditorias internas e revisões pela gestão para identificar oportunidades de melhoria e corrigir possíveis não conformidades.
- Monitorizar o desempenho do SGSI por meio de indicadores de desempenho e métricas de segurança da informação, avaliando a efetividade das medidas de proteção adotadas.
- Implementar um processo para identificar, avaliar e responder a incidentes de segurança, procurando aprender com eventos ocorridos e prevenir a recorrência de falhas.
- Manter-se atualizada com as alterações no cenário de ameaças e vulnerabilidades, bem como com novos requisitos regulatórios ou normativos.
- Fomentar uma cultura de segurança da informação entre os colaboradores da EIB, por meio de programas de sensibilização e formação regulares.
- Estabelecer canais de comunicação para receber feedback e sugestões das partes interessadas, incentivando a participação e a partilha de ideias.
- Realizar testes periódicos de segurança, como simulacros e testes de penetração, para avaliar a capacidade de resposta do SGSI e identificar áreas a melhorar.
- Documentar todas as ações de melhoria implementadas e os resultados obtidos, mantendo um histórico de modo a ser possível acompanhar o progresso do SGSI.

6.8.1 *Fator Humano*

Segundo Chopra e Chaudhary, 2020 os funcionários e colaboradores usam os sistemas diariamente e geralmente observam tudo a seu redor, podem partilhar questões que observam, coisas que talvez nunca se tenha pensado. Os relatórios de incidentes feitos por estes são uma das fontes mais valiosas para a melhoria contínua, normalmente os relatórios por eles realizados revelam falhas no sistema, sejam elas pequenas ou grandes.

É necessário que todos os funcionários, inclusive os recém-chegados à organização, estejam cientes da prática de relatar incidentes sempre que se verifiquem, nesse sentido

a organização deve efetuar ações regulares de sensibilização e consciencialização sobre segurança da informação.

Novos funcionários trazem experiências dos empregadores anteriores, como melhores práticas, ferramentas/tecnologias, entre outros, sendo importante fornecer aos novos funcionários as formas e meios para partilhar este tipo de informação.

6.8.2 *Novas Ferramentas/Tecnologias*

Quando é lançada uma nova tecnologia ou ferramenta relevante no mercado, é importante explorá-la para determinar se esta será útil para organização, devendo ser avaliado regularmente e decidir se vale a pena investir tempo e dinheiro em novas tecnologias, para se manter competitiva em relação aos seus concorrentes. Se existir investimento de tempo e recursos nesta abordagem, esta torna-se parte da implementação de melhorias (Chopra e Chaudhary, 2020).

As novas tecnologias podem desempenhar um papel fundamental na melhoria contínua de um SGSI, fornecendo recursos avançados e inovadores que podem fortalecer a segurança da informação e tornar o SGSI mais eficaz e eficiente. Algumas formas pelas quais essas ferramentas e tecnologias podem ser úteis incluem:

- Monitorização avançada
  Sistemas de deteção de intrusão, análise de tráfego e registos de eventos em tempo real, são exemplo disso (IDS/IPS, SIEM, NTA, EDR, etc.).
- Automação de processos
  Agilizar a resposta a incidentes e reduzir erros humanos.
- Análise de dados
  Soluções de análise de big data para identificar padrões e tendências de ameaças.
- Autenticação multi fator
  Reforçar a segurança de acessos aos sistemas e dados.
- Criptografia
  Proteger informações sensíveis e comunicações.

- Conformidade
  Ferramentas que auxiliem a garantir o cumprimento das políticas e normas de segurança.
- Testes de penetração
  Avaliar a robustez das defesas do sistema contra ataques.
- Formação de consciencialização
  Utilizar recursos educativos interativos para aumentar a cultura de segurança entre os colaboradores.

A segurança da informação vai muito além da adoção de tecnologias de ponta, como antivírus, firewalls, entre outras. Embora essas ferramentas sejam importantes e essenciais para proteger os ativos de informação, a verdadeira eficácia da segurança da informação reside numa abordagem holística que engloba a normalização de processos e a consciencialização dos diversos atores envolvidos no tratamento de ativos de informação. A organização deve manter um equilíbrio entre estes fatores, pois uma abordagem integrada ajuda a reduzir os riscos de incidentes, mitigar impactos e proteger a reputação e a continuidade dos negócios da organização.

6.8.3 *Leis e Regulamentos*

As leis e regulamentos devem ser rigorosamente seguidos; este facto não pode ser evitado. É necessário considerar não apenas as leis locais, mas também as leis internacionais, caso contrário, os produtos ou serviço poderão não ser aceites nos países de destino. Portanto, sempre que novas leis forem publicadas devem ser analisadas e todos os controlos de segurança implementados, estas ações devem ser identificadas como parte do acompanhamento e melhoria contínua (Chopra e Chaudhary, 2020).

Em Suma, as Leis e Regulamentos são um ponto crítico a ser considerado em todas as etapas da melhoria contínua de um SGSI, a conformidade com as leis, regulamentos e normas aplicáveis é fundamental para garantir que a organização esteja conforme as obrigações legais relacionadas com segurança da informação.

Ao realizar melhorias contínuas no SGSI, a organização deve levar em conta as leis e regulamentos relevantes que se aplicam ao seu setor, país ou região, podendo incluir leis

de proteção de dados, regulamentos de privacidade, legislação específica do setor, entre outros.

6.9 CONFORMIDADE COM METODOLOGIAS ADOTADAS

Com o propósito de avaliar o estado de implementação do projeto, será a seguir realizado um mapeamento das principais metodologias que nortearam este projeto. Isso inclui a análise dos documentos e registos obrigatórios da ISO/IEC 27001, bem como a verificação da conformidade com os passos delineados no roadmap estabelecido pela Integrity. Este exercício proporcionará uma visão do estado atual e garantirá a conformidade com as diretrizes estabelecidas.

6.9.1 *Documentos e registos obrigatórios da ISO/IEC 27001*

A Implementação de um SGSI desempenha um papel preponderante na proteção dos ativos de informação e dados numa organização. Para garantir a conformidade com os requisitos estabelecidos pela norma ISO/IEC 27001, é importante estabelecer uma estrutura que identifique de forma clara e abrangente os documentos e registos obrigatórios.

Segundo Ghazvini et al., 2018 a norma ISO/IEC 27001 Anexo A está dividido em três secções, documentos obrigatórios, registos obrigatórios e documentos não obrigatórios. A imagem 31 apresenta a estrutura dos controlos a serem utilizados pela organização para melhorar a segurança dos ativos de informação. (Note-se que os documentos do Anexo A são obrigatórios apenas se existirem riscos que exijam a sua implementação).

Mandatory documents required by ISO 27001:2013	Non-mandatory documents and records required by ISO 27001:2013	Mandatory records required by ISO 27001:2013
1. The scope of the ISMS (clause 4.3) 2. Information security policy and objectives (clauses 5.2 and 6.2) 3. Risk assessment and risk treatment methodology (clause 6.1.2) 4. Statement of Applicability (clause 6.1.3 d) 5. Risk treatment plan (clauses 6.1.3 e and 6.2) 6. Risk assessment report (clause 8.2) 7. Definition of security roles and responsibilities (clauses A.7.1.2 and A.13.2.4) 8. Inventory of assets (clause A.8.1.1) 9. Acceptable use of assets (clause A.8.1.3) 10. Access control policy (clause A.9.1.1) 11. Operating procedures for IT management (clause A.12.1.1) 12. Secure system engineering principles (clause A.14.2.5) 13. Supplier security policy (clause A.15.1.1) 14. Incident management procedure (clause A.16.1.5) 15. Business continuity procedures (clause A.17.1.2) 16. Statutory, regulatory, and contractual requirements (clause A.18.1.1)	1. Procedure for document control (clause 7.5) 2. Controls for managing records (clause 7.5) 3. Procedure for internal audit (clause 9.2) 4. Procedure for corrective action (clause 10.1) 5. Bring your own device (BYOD) policy (clause A.6.2.1) 6. Mobile device and teleworking policy (clause A.6.2.1) 7. Information classification policy (clauses A.8.2.1, A.8.2.2, and A.8.2.3) 8. Password policy (clauses A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, and A.9.4.3) 9. Disposal and destruction policy (clauses A.8.3.2 and A.11.2.7) 10. Procedures for working in secure areas (clause A.11.1.5) 11. Clear desk and clear screen policy (clause A.11.2.9) 12. Change management policy (clauses A.12.1.2 and A.14.2.4) 13. Backup policy (clause A.12.3.1) 14. Information transfer policy (clauses A.13.2.1, A.13.2.2, and A.13.2.3) 15. Business impact analysis (clause A.17.1.1) 16. Exercising and testing plan (clause A.17.1.3) 17. Maintenance and review plan (clause A.17.1.3) 18. Business continuity strategy (clause A.17.2.1)	1. Records of training, skills, experience, and qualifications (clause 7.2) 2. Monitoring and measurement results (clause 9.1) 3. Internal audit program (clause 9.2) 4. Results of internal audits (clause 9.2) 5. Results of the management review (clause 9.3) 6. Results of corrective actions (clause 10.1) 7. Logs of user activities, exceptions, and security events (clauses A.12.4.1 and A.12.4.3)

Figura 31: Documentos e registos da ISO/IEC 27001:2013 (Ghazvini et al., 2018)

Neste sentido tendo como base a imagem 31 definida acima, apresenta-se a tabela 12 de mapeamento que detalha como cada requisito obrigatório da ISO/IEC 27001 é abordado nos documentos do SGSI da EIB. No fundo, é uma tabela parecida com a Declaração de Aplicabilidade (SoA) mas resumida apresentando só documentos obrigatórios e estendida às cláusulas. Esta tabela permite uma análise da correspondência entre as exigências normativas e a abordagem adotada no SGSI da EIB, reforçando a conformidade, a transparência e a eficácia das práticas de segurança da informação implementadas.

Cláusula / Controlo	**Documento do SGSI da EIB**
Âmbito do SGSI **Cláusula 4.3**	4.3 - Âmbito do SGSI
Política de segurança da informação e objetivos **Cláusulas 5.2 e 6.2**	A.1 - Política Geral de Segurança da Informação

Contínua na próxima página...

Cláusula / Controlo	Documento do SGSI da EIB
Metodologias de análise e avaliação de risco e de tratamento de risco **Cláusula 6.1.2**	5.1 - Metodologia Gestão do Risco
Declaração de aplicabilidade **Cláusula 6.1.3.d**	4.10 - Declaração de Aplicabilidade (SoA)
Plano de tratamento de risco **Cláusulas 6.1.3 e e 6.2**	5.8 - Plano de tratamento de riscos
Relatório de análise de riscos **Cláusula 8.2**	5.7 - Relatório de análise de risco do SGSI
Definição de papéis e responsabilidades pela segurança **Controlos A.7.1.2 e A.13.2.4**	4.7 - Manual de Funções
Inventário de ativos **Controlo A.8.1.1**	5.3.4 - Inventários de ativos
Uso aceitável de ativos **Controlo A.8.1.3**	A.5 - Política de Gestão de Ativos
Política de controlo de acessos **Controlo A.9.1.1**	A.12 - Política de Controlo de Acessos Físicos A.6 - Política de Acesso e Controlo de Informação
Procedimentos operacionais para a gestão de TI **Controlo A.12.1.1**	4.9.3 - Procedimentos de TI
Princípios da engenharia de segurança de sistemas **Controlo A.14.2.5**	6.6 - Formação e Consciencialização 4.9 - Capitulo Políticas de segurança e procedimentos

Contínua na próxima página...

Cláusula / Controlo	Documento do SGSI da EIB
Política de segurança com fornecedores **Controlo A.15.1.1**	A.14 - Política de Relação com Fornecedores
Procedimento para a gestão de incidentes **Controlo A.16.1.5**	C.2 - Registo de Incidentes de segurança da informação
Procedimentos de continuidade de negócio **Controlo A.17.1.2**	Não Foram definidos procedimentos de continuidade de negócio no âmbito deste projeto
Requisitos estatutários, regulatórios e contratuais **Controlo A.18.1.1**	B.1 Leis e Normas Contratos com clientes, fornecedores, colaboradores, prestadores de serviços ou outras partes interessadas

Tabela 11: Mapeamento entre documentos obrigatários da norma ISO/IEC 27001 e documentos desenvolvidos no âmbito do SGSI da EIB

A seguir será apresentada a tabela que mapeia os documentos não obrigatórios, **que foram implementados** no âmbito do desenvolvimento do SGSI da EIB.

Cláusula / Controlo	Documento SGSI da EIB
Procedimento para controlo de documentos **Cláusulas 7.5**	4.6 - Gestão Documental
Procedimento para auditoria interna **Cláusula 9.2**	6.5 - Auditorias Internas
Política para uso de dispositivo pessoal (BYOD) **Controlo A.6.2.1**	B.10 - BYOD (Bring Your Own Device)

Contínua na próxima página...

Cláusula / Controlo	Documento SGSI da EIB
Política para dispositivos móveis e trabalho remoto **Controlo A.6.2.1**	B.9 - Trabalho Remoto
Política de classificação da informação **Controlos A.8.2.1, A.8.2.2 e A.8.2.3**	A.9 - Política de Classificação da Informação A.5 - Política de Gestão de Ativos A.10 - Política de Gestão e Eliminação de Suportes de Informação
Política de senhas **Controlos A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1 e A.9.4.3)**	A.6 - Política de Acesso e Controlo de Informação A.11 - Política de Controlo Criptográfico C.1 - Registo de Incidentes de segurança da informação
Política de descarte e destruição **Controlos A.8.3.2 e A.11.2.7**	A.10 - Política de Gestão e Eliminação de Suportes de Informação
Política de secretária limpa e écran limpo **Controlo A.11.2.9**	B.3 - Manutenção de Postos e Ambiente de Trabalho
Política de gestão de Alterações **Controlos A.12.1.2 e A.14.2.4**	A.8 - Política de Desenvolvimento de Software
Salvaguarda de informação (Backup) **Controlo A.12.3.1**	A.2 - Política de Backups e Recuperação
Política de transferência de informações **Controlos A.13.2.1, A.13.2.2 e A.13.2.3**	A.13 - Política de Transferência de informação

Tabela 12: Mapeamento entre documentos **não obrigatários** da ISO/IEC 27001 e documentos desenvolvidos no âmbito do SGSI da EIB

Não será realizado o mapeamento dos requisitos obrigatórios de registos, uma vez que, conforme mencionado anteriormente, o projeto encontra-se numa fase inicial e ainda não existem registos mensuráveis da sua implementação.

Através dos mapeamentos apresentados nas tabelas acima, verifica-se que grande parte dos requisitos obrigatórios e não obrigatórios foi abordada no desenvolvimento deste projeto de implementação de SGSI, o que demonstra o cumprimento normativo em relação à ISO/IEC 27001.

6.9.2 *Roadmap Integrity*

Este projeto tem como um dos seus objetivos o alinhamento com o roadmap apresentado pela (Integrity, 2023) para a implementação típica de um SGSI, incluindo os tempos necessários em cada fase do projeto, demonstrados na tabela 13.

Fase	**Tempo**
Preparação	1 a 2 meses
Diagnóstico	1 a 3 meses
Implementação	1 a 4 meses
Operação	3 a 6 meses

Tabela 13: Tempos definidos no roadmap Integrity

Além dos mapeamentos já feitos durante este projeto, a seguir será realizado na tabela 14 um mapeamento entre os documentos desenvolvidos durante o projeto de implementação do SGSI da EIB e as etapas definidas pela Integrity, a fim de demonstrar o cumprimento dos objetivos estabelecidos.

Fase	**Etapa**	**Descrição Integrity**	**Documento do SGSI**
Preparação	**1**	Obter suporte da gestão de topo	4.1 - Suporte da gestão de topo

Contínua na próxima página...

Fase	Etapa	Descrição Integrity	Documento do SGSI
Preparação	**1**	Procedimento de controlo documental	4.6 - Gestão Documental
Preparação	**2**	Definir o âmbito do SGSI	4.3 - Âmbito do SGSI
Preparação	**3**	Formação/Awareness	4.2 - Reuniões de Kickoff
Diagnostico	**4**	Análise de GAP	4.8 - Análise GAP
Diagnostico	**5**	Inventariar Ativos de Informação	5.3.4 - Inventários de ativos
Diagnostico	**6**	Definir metodologia de gestão de riscos	5.1 - Metodologia Gestão do Risco
Diagnostico	**7**	Avaliação de risco	5.6 - Matriz de riscos e Oportunidades
Diagnostico	**7**	Relatório de análise de risco	5.7 - Relatório de análise de risco do SGSI
Diagnostico	**8**	Plano de tratamento de riscos	5.8 - Plano de tratamento de riscos
Implementação	**9**	Definir política da segurança da Informação	A.1 - Política Geral de Segurança da Informação
Implementação	**10**	Documentar procedimentos de SGSI	4.9.3 - Procedimentos de TI
Implementação	**11**	Declaração de aplicabilidade (SoA)	4.10 - Declaração de Aplicabilidade (SoA)
Operação	**12**	Formação/Awareness	6.6 - Formação e Consciencialização
Operação	**14**	Ferramentas de operação do SGSI	5.11 - Gestão de incidentes de SI
Operação	**15**	Monitorização do SGSI	6.1 - Monitorização do SGSI

Contínua na próxima página...

Fase	Etapa	Descrição Integrity	Documento do SGSI
Operação	**15**	Métricas de SI	6.2 - Métricas e indicadores de SI
Operação	**16**	Revisão de cumprimento do SGSI	6.4 - Revisão do SGSI
Operação	**17**	Auditoria Interna	6.5 - Auditorias Internas

Tabela 14: Mapeamento entre roadmap Integrity e documentos desenvolvidos no SGSI

6.10 SÍNTESE

Neste capítulo, foram abordados temas fundamentais para a eficácia do SGSI da EIB. Através da Monitorização do SGSI, a organização garante uma vigilância constante dos processos e atividades relacionadas com a segurança da informação, identificando ameaças e vulnerabilidades.

As métricas e indicadores do SGSI fornecem uma visão objetiva e mensurável do desempenho do SGSI, permitindo avaliar o progresso relativamente às metas e objetivos estabelecidos.

Através das auditorias internas, a EIB realiza avaliações periódicas para assegurar a conformidade com as políticas e procedimentos estabelecidos, bem como identifica oportunidades de melhoria.

Na revisão do SGSI é realizada uma análise dos resultados das auditorias, métricas e indicadores, para tomar decisões estratégicas e direcionar a melhoria contínua do sistema.

A formação e consciencialização são fundamentais para garantir que todos os colaboradores estejam devidamente preparados e conscientes dos riscos de segurança da informação, contribuindo para a cultura de segurança da organização.

Os simulacros permitem testar a capacidade de resposta do SGSI em situações de incidentes reais, melhorando a preparação e prontidão da EIB para tratar eventos de segurança.

Finalmente, a melhoria contínua é um princípio chave que percorre todos os tópicos apresentados, impulsionando a EIB a evoluir e adaptar o seu SGSI constantemente, conforme a alterações no contexto de segurança e necessidades da organização.

Por fim é apresentado um mapeamento do roadmap apresentado pela Integrity para a implementação de um SGSI e os documentos desenvolvidos no projeto de implementação do SGSI da EIB e um mapeamento aos documentos obrigatórios na norma ISO/IEC 27001.

7

CONCLUSÕES

Neste projeto, foi abordada a implementação do Sistema de Gestão de Segurança da Informação (SGSI) na Empresa Industrial de Borracha, S.A. (EIB), reconhecendo-se a importância crítica da segurança da informação no cenário empresarial atual. Inicialmente, delineou-se o âmbito desse projeto, priorizando a melhoria da segurança da informação e a integração com os sistemas de gestão ISO 9001 e ISO 14001.

Os objetivos estabelecidos, além da implementação do SGSI, abrangeram três áreas-chave: Vantagem Competitiva, Segurança dos Sistemas e Conformidade Legal e Regulatória. procurou-se fortalecer a posição da EIB no mercado, proteger os seus sistemas contra ameaças e garantir a conformidade com regulamentações, incluindo o RGPD.

Este projeto representou um passo significativo na proteção dos ativos de informação da EIB e na promoção de uma cultura de cibersegurança. Apesar dos desafios encontrados, a EIB demonstrou estar determinada e empenhada a enfrentá-los e a prosseguir com a melhoria da segurança da informação num ambiente digital em constante evolução.

7.1 RESULTADOS ALCANÇADOS

O projeto de implementação do SGSI na EIB encontra-se ainda numa fase inicial, o que torna prematuro aferir resultados concretos. Contudo, já são visíveis avanços promissores que apontam para um reforço da segurança da informação, crescimento pessoal e preparação para próximas etapas do projeto:

1. Políticas e Procedimentos
   A implementação do SGSI, está a desenvolver uma estrutura robusta de políticas e procedimentos de segurança e operacionais, que visam estabelecer diretrizes claras para a utilização segura dos ativos de informação e a adoção de práticas consistentes e responsáveis em toda a organização.

2. Integração Progressiva com Sistemas Existentes
   O SGSI está a ser integrado de forma gradual e coesa com os sistemas de gestão já existentes na EIB, tais como as normas ISO 9001 e ISO 14001. Esta integração visa otimizar os processos e aproveitar sinergias para uma gestão mais eficaz.

3. Cultura e Consciencialização Emergente
   A implementação do SGSI tem desencadeado uma mudança cultural, com uma consciencialização crescente de todos sobre a importância da segurança da informação, especialmente na gestão de topo e nos quadros que integraram as reuniões de arranque. Já foram efetuadas ações de sensibilização que estão a contribuir para uma abordagem mais responsável relativamente aos ativos de informação, proporcionando também um enriquecimento pessoal ao ampliar os conhecimentos em cibersegurança.

4. Preparação para Certificação Futura
   Embora não seja um objetivo imediato, o projeto está a criar as bases para uma eventual certificação ISO/IEC 27001. A EIB está a estruturar-se para cumprir os requisitos dessa certificação e demonstrar compromisso com as melhores práticas de segurança.

5. Fundamentos para a Gestão de Riscos e Ativos:
   A fase inicial do projeto já engloba a definição de abordagens para a gestão de riscos e ativos, em conformidade com a norma ISO/IEC 27005, estabelecendo uma base sólida para futuras avaliações de riscos, incluindo o registo e a resposta a incidentes de segurança.

Apesar de numa fase inicial, os primeiros passos na implementação do SGSI na EIB demonstram um compromisso com a segurança da informação, o enriquecimento pessoal dos colaboradores e a sensibilização para os desafios inerentes. Esta etapa inicial destaca-se a integração com sistemas de gestão já existentes, pela preparação futura para certificação e pela construção de alicerces sólidos para implementação de mais controlos de segurança, políticas e procedimentos e uma gestão de riscos eficaz. Os primeiros sinais refletem uma jornada contínua de fortalecimento da segurança da informação e melhoria contínua, beneficiando tanto a organização como o desenvolvimento profissional dos envolvidos.

7.2 ANALISE CRITICA

A análise crítica da implementação do SGSI na EIB revela desafios e obstáculos que podem impactar negativamente o sucesso do projeto, alguns pontos de reflexão são:

1. Colocar em standby projetos de segurança da informação
   A segurança da informação é frequentemente negligenciada ou deixada em segundo plano por diversas razões, como a priorização de outros projetos ou falta de compreensão sobre a importância da proteção dos ativos de informação, esta atitude pode expor a organização a riscos significativos, especialmente num cenário cada vez mais digital, interligado e globalizado.
2. Compreensão limitada sobre segurança da informação
   A segurança da informação vai além da implementação de ferramentas tecnológicas, pois abrange conceitos, boas práticas e comportamentos. A consciencialização e o compromisso de todos é essencial para fortalecer a cultura de segurança e reduzir os riscos de violações e incidentes.
3. Equilibrar projetos de segurança e projetos produtivos
   Muitas organizações enfrentam dificuldades em dar a devida importância a projetos de segurança da informação, especialmente quando comparados com projetos produtivos, essa falta de equilíbrio pode levar a lacunas na proteção dos ativos de informação e comprometer a resiliência da organização perante ameaças cibernéticas.
4. Desafios na obtenção de investimentos preventivos
   A segurança da informação exige investimentos em medidas preventivas para mitigar riscos e evitar incidentes. No entanto, a tendência das organizações é, na maioria das vezes, investir em ações corretivas, após a ocorrência dos incidentes. A abordagem reativa, no caso de violações de segurança, por norma, resulta em custos e impactos significativos e desnecessários.

7.3 CONSIDERAÇÕES

O projeto de implementação do SGSI na EIB representa um marco inicial e relevante pela procura de altos padrões em segurança da informação. Embora existam alguns detalhes

a serem melhorados, o objetivo principal foi alinhar o SGSI com a norma ISO/IEC 27001:2013, que norteou todas as etapas do processo. O foco principal foi estabelecer uma base sólida para a proteção dos ativos de informação, garantindo confidencialidade, integridade e disponibilidade.

Durante esta etapa, foram seguidos os requisitos da ISO/IEC 27001:2013, apesar de ter sido disponibilizada a versão ISO/IEC 27001:2022 durante a execução deste projeto, adaptando-os à realidade e necessidades da EIB. Embora estejamos numa fase inicial de implementação, o compromisso com a melhoria contínua é constante, mas inviabilizando o cumprimento de alguns requisitos da norma, nomeadamente aqueles que requerem uma avaliação da implementação efetiva e cimentada do SGSI.

O crescimento e aperfeiçoamento seguramente ocorrerão ao longo do tempo, evoluindo e amadurecendo o SGSI, findo esse período, naturalmente poderá ser requerida pela EIB a certificação.

Nesta jornada, foi fortalecida a governança dos sistemas de TI da EIB e consciencializada toda a organização sobre a importância da cibersegurança. A cultura de segurança da informação está a passar por uma transformação significativa, e a adoção de medidas de segurança tornou-se uma prática normalizada, proporcionando maior resiliência e proteção contra ameaças emergentes.

7.4 TRABALHO FUTURO

Tendo em vista fortalecer a postura de segurança da informação, responder de forma proativa às ameaças emergentes e garantir a proteção contínua dos dados e informações críticas da EIB alguns trabalhos futuros podem ser considerados:

1. Desenvolvimento de um Plano de Recuperação de Desastres
   Elaborar um plano detalhado para garantir a continuidade dos negócios e a rápida recuperação de incidentes graves, minimizando o impacto nas operações da EIB.
2. Implementação de Controlos Adicionais
   Identificar áreas de risco e implementar controlos de segurança adicionais para fortalecer ainda mais a proteção dos ativos de informação da EIB.

3. Obtenção da Certificação ISO/IEC 27001
   Considerar a certificação ISO/IEC 27001 como um objetivo a médio prazo, demonstrando o compromisso da EIB em cumprir as melhores práticas de segurança da informação e obter uma vantagem competitiva e uma relação de confiança reforçada com os nossos clientes.
4. Realização de Auditorias de Segurança
   Realizar auditorias de segurança regulares para avaliar a eficácia dos controlos implementados, identificar possíveis vulnerabilidades e garantir a conformidade contínua com a ISO/IEC 27001.
5. Adoção de Tecnologias Emergentes
   A implementação de sistemas centralizados de logs ou um SIEM ou SOAR, bem como a consideração da implementação de honeypots e canarytokens. Avaliar e implementar tecnologias emergentes, como machine learning, inteligência artificial e IDS/IPS, para melhorar a deteção de ameaças e reforçar a cibersegurança da EIB.
6. Realização de Simulacros e Testes de Penetração
   Realizar exercícios regulares de simulação de incidentes e testes de penetração para avaliar a prontidão e a eficácia das medidas de segurança e identificar áreas de melhoria.

SEGURANÇA DA INFORMAÇÃO *"UMA JORNADA, NÃO UM DESTINO"*

Como afirmou Bruce Schneier, um dos maiores especialistas em segurança da informação do nosso tempo: *"A segurança é uma jornada, não um destino"*. Ao implementarmos o Sistema de Gestão de Segurança da Informação (SGSI) na EIB com dedicação e compromisso, reconhecemos que a proteção dos ativos de informação é uma jornada contínua e a garantia de que estamos preparados para enfrentar desafios em constante mutação. À medida que avançamos nesta jornada, reafirmamos o compromisso com a segurança, a integridade e a confidencialidade dos dados da organização. O SGSI é uma âncora de confiança, que nos ajudará a enfrentar o futuro com resiliência e perseverança.

BIBLIOGRAFIA

Axelos (2023). *ITIL (Information Technology Infrastructure Library)*. URL: https://www.axelos.com/best-practice-solutions/itil.

Bastos, Alberto (2022). *A nova ISO 27005 para gestão de riscos de segurança da informação*. URL: https://www.linkedin.com/pulse/nova-iso-27005-para-gest%C3%A3o-de-riscos-seguran%C3%A7a-da-alberto-bastos/.

Calder, Alan (2009). *Information Security based on ISO 27001 / ISO 27002 -A Management Guide*. Van Haren Publishing, Zaltbommel. ISBN: 978 90 8753 540 7. URL: http://www.vanharen.net.

Carvalho, Carla e Eduardo Marques (2019). «Adapting ISO 27001 to a Public Institution». Em: *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1–6. DOI: 10.23919/CISTI.2019.8760870.

Centro Nacional de Cibersegurança (2023). *Guia de Gestão dos Riscos*. URL: https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf.

Chopra, Abhishek e Mukund Chaudhary (2020). *Implementing an Information Security Management System*. Apress. DOI: 10.1007/978-1-4842-5413-4. URL: https://doi.org/10.1007%2F978-1-4842-5413-4.

Correia, Carlos Manuel Rosa (2016). «Plano de Implementação da Norma ISO/IEC 27001 no INEM». Universidade Nova de Lisboa.

Decreto-Lei n.º 55/2019 (2019). Diário da República n.º 92/2019, Série I. URL: https://diariodarepublica.pt/dr/detalhe/decreto-lei/55-2019-122157759.

despnet (2023). *Ciclo de Vida de Serviço: Conheça o Modelo*. URL: https://www.despnet.com/ciclo-de-vida-servico-conheca-o-modelo/.

Everett, Cath (jan. de 2011). «Is ISO 27001 worth it?» Em: vol. 2011, pp. 5–7. DOI: 10.1016/S1361-3723(11)70005-7.

Ferreira, Alexandre José Henriques (2020). «Implementação de um sistema de gestão de segurança da informação em conformidade com a ISO/IEC 27001». Universidade de Coimbra.

NP ISO 9001 (2015). *Gestão da Qualidade*. pt. Standard. ASSOCIAÇÃO PORTUGUESA PARA A QUALIDADE.

NP ISO 31000 (2012). *Gestão do Risco*. pt. Standard. ASSOCIAÇÃO PORTUGUESA PARA A QUALIDADE. URL: https://apq.pt/iso-31000-gestao-do-risco/.

Ghazvini, Arash, Zarina Shukur e Zaihosnita Hood (2018). «Review of information security policy based on content coverage and online presentation in higher education». Em: *International Journal of Advanced Computer Science and Applications* 9.8.

Hsu, Carol, Tawei Wang e Ang Lu (2016). «The Impact of ISO 27001 Certification on Firm Performance». Em: *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pp. 4842–4848. DOI: 10.1109/HICSS.2016.600.

Hudson, John e Marta Orviska (2013). «Firms' adoption of international standards: One size fits all?» Em: *Journal of Policy Modeling*, pp. 289–306. ISSN: 0161-8938. DOI: https://doi.org/10.1016/j.jpolmod.2012.04.001. URL: https://www.sciencedirect.com/science/article/pii/S0161893812000397.

IBM (2023). *Recursos da IBM sobre NIST*. URL: https://www.ibm.com/br-pt/topics/nist.

Integrity (2023). *Iso 27001.pt*. URL: https://www.xzconsultores.pt/publicacoes/1/321-a-np-iso-iec-270012013-sistema-de-gestao-de-seguranca-da-informacao.

ISACA (2023). *COBIT (Control Objectives for Information and Related Technologies)*. URL: https://www.isaca.org/resources/cobit.

ISO/IEC 27000 (2018). *Information technology - Security techniques - Information security management systems - Overview and vocabulary*. en. Standard. International Organization for Standardization. URL: https://www.iso.org/standard/73906.html.

ISO/IEC 27001 (2013). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. en. Standard. International Organization for Standardization. URL: https://www.iso.org/standard/82875.html.

ISO/IEC 27701 (2019). *Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines*. en. Standard. International Organization for Standardization. URL: https://www.iso.org/standard/71670.html.

ISO/IEC 27002 (2022). *Information security, cybersecurity and privacy protection - Information security controls*. en. Standard. International Organization for Standardization. URL: https://www.iso.org/standard/75652.html.

ISO/IEC 27003 (2017). *Information technology - Security techniques - Information security management systems - Guidance*. en. Standard. International Organization for Standardization. URL: https://www.iso.org/standard/63417.html.

ISO/IEC 27005 (2022). *Information security, cybersecurity and privacy protection - Guidance on managing information security risks*. en. Standard. International Organization for Standardization. URL: https://www.iso.org/standard/80585.html.

ISO 31000 (2018). *Risk management — Guidelines*. en. Standard. International Organization for Standardization. URL: https://www.iso.org/standard/65694.html.

itsmnapratica (2023). *Conceitos COBIT 5*. URL: https://www.itsmnapratica.com.br/conceitos-cobit-5/.

Kosutic, Dejan (2023). *ISO 27001 2013 vs. 2022 revision – What has changed?* URL: https://advisera.com/27001academy/blog/2022/02/09/iso-27001-iso-27002/.

Lei do Cibercrime (2009). Diário da República n.º 178/2009, Série I. URL: https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2009-128879174.

Lei n.º 46/2018 (2018). Diário da República n.º 171/2018, Série I. URL: https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384.

Martins, José Carlos Lourenço (2021). *Gestão da Segurança da Informação e Cibersegurança nas Organizações - Sistemas e Método*. Silaba & Desafios. ISBN: 978-989-8842-59-6.

Al-Mayahi, Ibrahim e P Mansoor Sa'ad (2012). «Iso 27001 gap analysis-case study». Em: *Proceedings of the International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science, Computer ...

Muñoz, Johanna Carolina Ararat (2018). «Diseño de un SGSI Basado en la Norma ISO 27001 para la Empresa MA PEÑALOSA CÍA. S.A.S». Universidad Nacional Abierta y a Distancia Escuela De Ciencias Básicas, Tecnología e Ingeniería.

NIST (2023). *NIST Cybersecurity Framework Perspectives*. URL: https://www.nist.gov/cyberframework/perspectives.

Oliveira, Rui Manuel Campos (2015). «Contribuição para a estruturação do sistema integrado de gestão do grupo Cooprofar - Medlogcom integração da gestão de segurança da informação». Universidade Lusíada.

Ramos, Maria Augusta (2022). *A nova ISO 27005 para gestão de riscos de segurança da informação*. URL: https://www.xzconsultores.pt/publicacoes/1/321-a-np-iso-iec-270012013-sistema-de-gestao-de-seguranca-da-informacao.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (2016). URL: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02016R0679-20160504.

Sá Martins, Alexandre Gil de (2020). «Visualization of Security in Industrial Control Systems respecting IEC-62443». ISCTE, Instituto Universitário de Lisboa.

Santos, Joaquim Manuel Pires dos (2016). «Definição de Política de Segurança Informática no IPCB». Instituto Politécnico de Catelo Branco, Escola Superior de Tecnologia.

NIST SP 800-53 (2020). *Security and Privacy Controls for Federal Information Systems and Organizations*. Standar NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of Dec. 10, 2020, 2020. Gaithersburg, MD: National Institute of Standards e Technology. DOI: 10.6028/NIST.SP.800-53r5.

Ta-Seen, Junaid (2023). «ISO 27001: Information Security Management Systems». Em: pp. 1–5. DOI: 10.13140/RG.2.2.36267.52005.

NP ISO 14001 (2015). *Sistemas de gestão ambiental*. pt. Standard. ASSOCIAÇÃO PORTUGUESA PARA A QUALIDADE.

ISA/IEC 62443 (2020). *Sistemas de gestão ambiental*. en. Standard. International Society of Automation. URL: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

Smulders., Andre et al. (2018). *Fundamentos de Segurança ca Informação com base na ISO 27001 e na ISO 27002*. Brasport. ISBN: 0471491101.

Su., Hung-Chung, Suvrat Dhanorkar. e Kevin Linderman (2015). *A competitive Advantage from the Implementation Timing of ISO Management Standards*. Journal of Operations Management. DOI: https://doi.org/10.1016/j.jom.2015.03.004.

Zúquete, André (2018). *Segurança em redes informáticas*. Ed. por FCA.

APÊNDICES

A

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

A.1 POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

POLÍTICA DE SI **POL-SI-001.0**

POLÍTICA GERAL **APROVADO**

Criação 2023-04-18 **Aprovação** 2023-06-19

Introdução

A EIB - Empresa Industrial de Borracha reconhece a importância da proteção das informações que processa, armazena e transmite, e está comprometida em assegurar a confidencialidade, integridade e disponibilidade dessas informações. Esta Política de Segurança da Informação pretende estabelecer as diretrizes e princípios que devem ser seguidas por todos os funcionários, fornecedores e outros colaboradores da empresa para garantir a segurança da informação.

Âmbito

Esta política aplica-se a todas as informações, sistemas e equipamentos da EIB, independentemente da sua localização ou forma de processamento, incluindo todas as informações físicas, eletrónicas e verbais.

Responsabilidades

1. A Direção e Gestão de topo é responsável pela definição da política de segurança da informação e deve garantir que ela seja implementada e monitorizada em toda a organização.
2. Cada funcionário é responsável por cumprir esta política e reportar qualquer violação de segurança ou incidente à equipa de segurança da informação da empresa. incluindo a proteção de informações confidenciais e o uso responsável dos recursos de TI.
3. O departamento de TI é incumbido da implementação e manutenção dos controlos de segurança da informação estabelecidos pela política de segurança da informação. É responsável pela instalação e atualização de dispositivos de segurança, a exemplo de firewalls e antivírus, bem como a aplicação de patches e atualizações de software.
4. O departamento de segurança da informação é responsável por gerir a segurança da informação em toda a empresa, incluindo a análise de riscos, a implementação de controlos de segurança e gestão de incidentes de segurança. Deve também garantir que os colaboradores estejam cientes das políticas e procedimentos de segurança da informação aplicáveis.

Diretrizes

1. **Acesso à Informação**
    - O acesso à informação deve ser restrito apenas aos colaboradores que necessitam do acesso para desempenhar as suas funções.
    - O acesso a informações sensíveis deve ser controlado por meio de autenticação e autorização adequada.
    - O acesso a informações por fornecedores, parceiros e outros terceiros deve ser concedido apenas com autorização prévia da Direção e Gestão.
    - O acesso a áreas restritas da empresa, onde informações sensíveis ou críticas estão e são armazenadas, deve ser controlado e monitorizado.

- Os direitos de acesso de cada utilizador devem ser revistos regularmente para garantir que possam aceder apenas aos recursos necessários para desempenhar as suas funções. O acesso a recursos não utilizados deve ser removido.
- O uso de contas de administrador deve ser restrito apenas aos utilizadores que precisam desses direitos para desempenhar as suas funções. Os utilizadores com contas de administrador devem usar essas contas com precaução e apenas quando necessário.

2. **Proteção de Informações**

- Informações sensíveis devem ser classificadas e protegidas conforme o grau de confidencialidade.
- Todos os dispositivos de armazenamento de dados sensíveis devem ser encriptados e protegidos por senha.
- Todos os documentos físicos contendo informações sensíveis devem ser armazenados em armários fechados e protegidos com chave.
- A equipa de TI deve implementar mecanismos de criptografia para proteger informações confidenciais em trânsito e armazenada. As políticas de criptografia devem ser alinhadas às regulamentações e padrões relevantes e revistas regularmente.
- Os colaboradores devem ser formados e orientados a reconhecer possíveis ameaças à segurança da informação, incluindo phishing, malware, engenharia social e outras técnicas de ataque comuns e devem ser incentivados a reportar atividades suspeitas imediatamente.
- A equipa de segurança da informação deve realizar testes regulares de penetração em sistemas e infraestrutura para identificar possíveis vulnerabilidades e ameaças.
- Deve ser implementado um sistema de gestão de acessos que restrinja o acesso a informações confidenciais e que permita acesso somente a colaboradores autorizados. O sistema deve ser revisto periodicamente para garantir que as permissões de acesso estejam atualizadas e conforme as políticas de segurança da informação.

- A empresa deve implementar uma política de backup e recuperação de dados que inclua backups regulares e armazenamento seguro de dados críticos. Deve ser estabelecido um procedimento de recuperação em caso de falha de sistemas ou perda de dados.

3. **Uso de Equipamentos e Recursos de TI**

   - Os equipamentos e recursos de TI da empresa serão apenas para o desempenho de funções laborais.
   - O download, instalação ou o uso de software não autorizado nos dispositivos da empresa está estritamente proibido. Os colaboradores devem obter aprovação prévia da equipa de TI antes de instalar qualquer software nos sistemas da empresa.
   - Os colaboradores devem manter os seus dispositivos de TI pessoais separados dos equipamentos de TI da empresa.
   - Os colaboradores devem garantir a boa utilização e limpeza dos equipamentos e recurso de TI da empresa.
   - Os dispositivos de TI da empresa, como computadores, portáteis e smartphones, devem ser protegidos com senhas fortes e atualizadas regularmente. A equipa de TI deve implementar políticas de senha que atendam a requisitos mínimos de complexidade e comprimento.
   - É proibido a partilha de senhas de acesso a sistemas, dispositivos ou contas de utilizador. Cada utilizador é responsável por manter as suas credenciais de acesso confidenciais e não as pode divulgar.
   - O acesso remoto aos recursos de TI da empresa deve ser realizado somente por meio de conexões seguras e autorizadas. Os colaboradores devem utilizar redes privadas virtuais (VPN) ou outros mecanismos aprovados para estabelecer conexões seguras de acesso remoto.
   - O uso de dispositivos de armazenamento externo, como pen drives ou discos externos, deve ser restrito e controlado. Antes de conectar esses dispositivos aos sistemas da empresa, estes devem ser verificados pela equipa de TI quanto à presença de malware ou outras ameaças de segurança.

- Os colaboradores devem estar cientes das políticas de uso aceitável dos recursos de TI da empresa. O uso de sistemas de informação da empresa para atividades pessoais deve ser mínimo e restrito aos limites estabelecidos pela empresa.

4. **Gestão de Incidentes de Segurança da Informação**

   - Todos os incidentes de segurança da informação devem ser relatados imediatamente à equipa de segurança da informação da empresa.
   - Todos os incidentes devem ser investigados e documentados conforme os procedimentos da empresa.
   - Devem ser tomadas medidas para remediar quaisquer vulnerabilidades ou falhas de segurança identificadas.
   - A equipa de segurança da informação deve manter registos de todos os incidentes de segurança da informação, incluindo detalhes do incidente, ações tomadas, tempo de resposta e impacto.
   - A equipa de segurança da informação deve conduzir análises de vulnerabilidades periodicamente para identificar e mitigar possíveis falhas de segurança em sistemas e infraestrutura
   - A equipa de segurança da informação deve manter atualizadas as informações de contacto dos membros da equipa, bem como dos principais stakeholders, para garantir uma rápida e eficaz resposta em caso de incidentes de segurança.
   - Deve ser realizada uma revisão periódica dos procedimentos de gestão de incidentes de segurança da informação, a fim de garantir que estes estejam atualizados e adequados à natureza das atuais ameaças.
   - A equipa de segurança da informação deve garantir que todos os incidentes de segurança da informação sejam comunicados às partes interessadas relevantes em tempo útil, conforme as políticas e regulamentos aplicáveis.

Conclusão

A EIB reconhece que a segurança da informação é um elemento chave para o sucesso do negócio. Esta Política de Segurança da Informação estabelece diretrizes para proteger as informações sensíveis da empresa, garantindo a confidencialidade, integridade e disponibilidade dessas informações. Todos os funcionários, fornecedores e outros colaboradores da empresa devem seguir as políticas e procedimentos estabelecidos, visando proteger a segurança da informação em toda a empresa.

É importante destacar que a segurança da informação é uma responsabilidade partilhada por todos, desde a gestão de topo até aos funcionários de todos os níveis hierárquicos, cada um tem a responsabilidade de agir de forma responsável e segura ao manipular informações sensíveis e recursos de TI.

Com a implementação da Política de Segurança da Informação, a EIB pretende garantir a confiança dos seus clientes e parceiros, além de cumprir as obrigações legais e regulamentos aplicáveis à proteção de informações sensíveis, através de uma estratégia proativa e contínua, a empresa poderá reduzir os riscos de incidentes de segurança da informação e proteger a integridade dos seus dados e sistemas.

A.2 POLÍTICA DE BACKUPS E RECUPERAÇÃO

POLÍTICA DE SI **POL-SI-002.0**

BACKUPS E RECUPERAÇÃO **APROVADO**

Criação 2023-04-26 **Aprovação** 2023-06-19

Introdução

A Empresa Industrial de Borracha (EIB) reconhece a importância crítica dos dados e informações para a continuidade do seu negócio. Nesse contexto, a implementação de uma política de backups e recuperação eficiente e abrangente torna-se essencial para garantir a disponibilidade, a integridade e a recuperação dos dados em caso de perdas, falhas ou incidentes. A presente política estabelece as diretrizes e responsabilidades relacionadas com backups de dados na EIB, abrangendo Computadores pessoais, Servidores Intel, Servidores IBM System I e Sistemas de bases de dados.

A política de backups e recuperação da EIB visa assegurar que todos os dados relevantes sejam salvaguardados de forma adequada, minimizando o risco de perdas irreparáveis e garantindo a rápida recuperação em situações adversas. A equipa de Tecnologia da Informação (TI) é responsável por implementar, gerir e monitorizar os backups, assegurando que todos os procedimentos e práticas estejam em conformidade com as diretrizes estabelecidas.

Âmbito

A política de backups e recuperação define as diretrizes para a realização de backups de dados na EIB, abrangendo computadores pessoais, servidores, IBM AS400 e bases de dados.

Responsabilidades

A responsabilidade pela implementação, gestão e cumprimento dos backups está a cargo do Departamento de TI da EIB.

1. Departamento de TI
    a) Configurar, automatizar e monitorizar os backups em todos os dispositivos e sistemas abrangidos por esta política.
    b) Realizar testes regulares dos backups para verificar a sua efetividade e a capacidade de recuperação dos dados.
    c) Gerir o armazenamento dos backups, garantindo a integridade e a disponibilidade dos dados de forma segura.
    d) Monitorizar o processo de sincronização dos backups com a cloud, assegurando a redundância e a recuperação dos dados em caso de falhas ou desastres.
    e) Configurar, automatizar e executar os backups do sistema IBM AS400, garantindo a proteção e a recuperação dos dados do sistema.
    f) Realizar backups integrais dos sistemas regularmente, além dos backups incrementais ou diferenciais, para garantir a recuperação completa dos sistemas em caso de necessidade.
    g) Documentar e manter registos atualizados dos procedimentos de backup, incluindo detalhes sobre a configuração, frequência e armazenamento dos backups.
    h) Realizar auditorias periódicas para garantir a implementação e o cumprimento efetivo das diretrizes de backups.
2. Utilizadores
    a) Garantir que guarda os ficheiros e dados relevantes nas áreas abrangidas pelos backups automáticos, áreas de utilizadores (Os meus documentos e Ambiente de trabalho).
    b) Colaborar com o departamento de TI ao fornecer acesso aos dispositivos e sistemas para a configuração e realização dos backups.

c) Seguir as diretrizes e políticas de segurança da informação, garantindo a integridade e a disponibilidade dos dados antes do processo de backup.

d) Informar imediatamente o departamento de TI sobre quaisquer problemas, falhas ou perdas de dados para que ações corretivas possam ser tomadas.

Sistemas Abrangidos

1. Computadores Pessoais

   Será salvaguardada a área de utilizadores (Os meus documentos e Ambiente de trabalho) com roaming profiles, garantindo a proteção e a recuperação dos dados importantes dos utilizadores em caso de perda ou falha do dispositivo.

2. Servidores Intel

   Os backups serão realizados de hora em hora utilizando técnicas de Volume Shadow Copy Service (VSS), assegurando a consistência dos dados e minimizando o impacto nas operações em andamento.

3. Servidores IBM System I

   Os backups serão realizados diariamente em fitas magnéticas (tapes), com limite de 6 tapes uma por dia alternando a de sexta-feira, além disso, será realizada uma cópia para os servidores NAS. Esta prática garante a proteção e a recuperação dos dados do sistema AS400 e algum tipo de redundância.

4. Sistemas de bases de dados

   O backup das bases de dados será realizado individualmente e armazenado em sistema de NAS, considerando a periodicidade adequada para cada base de dados. Esta abordagem garante que seja possível recuperar bases de dados individualmente, sem a necessidade de restaurar todo o sistema. Dessa forma, as informações contidas em cada base de dados podem ser protegidas de forma mais eficiente e os processos de recuperação podem ser executados de forma ágil e direcionada.

Armazenamento

1. Dispositivos

   Os backups serão mantidos em servidores NAS deslocalizados e alguns localizados dentro de cofre antifogo, bem como as fitas magnéticas (tapes), visando garantir a disponibilidade e a segurança dos dados em caso de incidentes físicos.

2. Sincronização com a nuvem

   Os servidores NAS terão rotinas de sincronização de pastas com armazenamento na nuvem, garantindo a redundância dos dados e facilitando a recuperação em caso de falhas ou desastres nos servidores locais. Deste modo permite que os dados sejam copiados e armazenados simultaneamente nos servidores NAS e na nuvem, proporcionando uma camada adicional de proteção e possibilitando a recuperação dos dados de forma mais rápida e eficiente em situações adversas.

3. Taxa de retenção

   Uma taxa de retenção adequada para os backups na EIB é de 1 mês, significa que os backups serão mantidos por um período de 30 dias. Essa taxa de retenção é estabelecida considerando as necessidades operacionais da EIB, garantindo a disponibilidade de versões anteriores dos dados dentro do intervalo de tempo.

Conclusão

Esta política de backups pretende proteger os dados críticos da EIB, garantindo a disponibilidade e a recuperação desses dados em caso de perda, falha ou incidentes, a equipa de TI tem a responsabilidade de implementar, seguir e testar regularmente as diretrizes, assegurando a correta realização dos backups, a integridade dos dados e a efetividade dos processos de recuperação.

A.3 POLÍTICA DE REDES

POLÍTICA DE SI **POL-SI-003.0**

REDES **APROVADO**

Criação 2023-04-26 **Aprovação** 2023-06-19

Introdução

A EIB reconhece a importância da infraestrutura de rede como elemento fundamental para o suporte das suas operações e para a segurança das suas informações. Esta Política de Rede estabelece as diretrizes e os procedimentos que devem ser seguidos por todos os colaboradores, fornecedores e parceiros de negócios da EIB relativamente ao uso da rede.

Âmbito

Esta política abrange todos os aspetos relacionados à infraestrutura de rede da EIB, incluindo redes com fio e sem fio, conexões à Internet, rede interna, rede de convidados, acessos VPN e outros recursos de rede utilizados pela empresa.

Responsabilidades

1. Direção e Gestão
   A Direção Executiva da EIB é responsável por:
   - Definir e aprovar a política de rede da empresa.
   - Assegurar o cumprimento das diretrizes estabelecidas nesta política.
   - Fornecer recursos adequados para a implementação e manutenção da infraestrutura de rede.

- Promover a consciencialização sobre segurança da rede e a importância do cumprimento desta política.

2. Departamento de TI
   O Departamento de TI da EIB é responsável por:
   - Gerir e manter a infraestrutura de rede, incluindo servidores, switches, routers e demais componentes de rede.
   - Configurar e monitorizar as políticas de segurança de rede, como firewalls, sistemas de deteção de intrusões e filtros de conteúdo.
   - Realizar backups regulares das configurações das redes e implementar medidas de recuperação de desastres para a infraestrutura de rede.
   - Garantir a disponibilidade, confiabilidade e desempenho da rede.
   - Manter-se atualizado relativamente às melhores práticas de segurança de rede e implementar medidas de proteção adequadas.
3. Colaboradores e utilizadores
   Todos os colaboradores e utilizadores das redes da EIB têm a responsabilidade de:
   - Utilizar a rede de forma responsável, seguindo as políticas, diretrizes e procedimentos estabelecidos.
   - Proteger as informações confidenciais e sensíveis da empresa, evitando a divulgação não autorizada.
   - Não realizar atividades que possam comprometer a segurança da rede ou violar as políticas de uso aceitável.
   - Informar imediatamente ao Departamento de SI sobre qualquer incidente de segurança ou violação suspeita.

Infraestrutura de Rede

A infraestrutura de rede da EIB será mantida e atualizada regularmente pelo Departamento de TI, inclui a configuração adequada de switches, routers, firewalls e outros

dispositivos de rede, além da implementação de medidas de segurança, como autenticação de utilizadores, segmentação de redes e criptografia.

Rede Wireless

A EIB disponibilizará acesso à rede wireless para os colaboradores autorizados. O uso da rede wireless deve seguir as diretrizes de segurança estabelecidas, como a utilização de autenticação segura, criptografia de dados e restrições de acesso.

Rede de Convidados

A EIB disponibiliza uma rede separada para colaboradores e convidados, com acesso controlado e limitado à Internet.

Acessos Externos

Os colaboradores da EIB e fornecedores externos que necessitem de acesso à rede interna da empresa a partir de locais remotos devem utilizar uma conexão segura, como uma VPN (Rede Virtual Privada). A utilização da VPN deve seguir as diretrizes de segurança estabelecidas, incluindo autenticação de utilizadores, criptografia de dados e políticas de acesso restrito.

Monitorização e Auditoria

O Departamento de TI realizará uma monitorização contínua da rede para identificar possíveis ameaças, atividades suspeitas ou violações de segurança. Serão implementadas ferramentas de monitorização, registo de logs e auditorias regulares para garantir a conformidade com as políticas e detetar possíveis incidentes de segurança.

Segregação de redes

As redes internas da EIB devem ser segmentadas em zonas de segurança com base nas necessidades e requisitos específicos. Cada zona de segurança deve possuir controlos de acesso adequados para restringir o tráfego entre as diferentes redes. Aplicar o principio "Zero Trust Network", onde apenas o acesso necessário é concedido, reduzindo assim o risco de exposição.

Consciencialização e Treino

A EIB promoverá programas de treino e consciencialização em segurança de redes para todos os colaboradores e utilizadores da empresa. O conteúdo desses programas incluirá a disseminação de informações sobre melhores práticas de segurança, políticas de uso aceitável, identificação de ameaças e como registar incidentes de segurança.

Cumprimento e Consequências

O não cumprimento desta Política de Rede poderá resultar em medidas disciplinares, conforme as políticas internas da EIB. Podendo incorrer em advertências, suspensões ou até mesmo rescisão do contrato de trabalho, ou parceria.

Conclusão

A EIB reforça a importância de todos os colaboradores e utilizadores cumprirem esta política para garantir a segurança e a integridade da rede, bem como a proteção das informações confidenciais da empresa.

Esta Política de Rede é parte integrante das políticas de segurança da informação da EIB e está sujeita a revisões periódicas para garantir a sua eficácia e conformidade com as melhores práticas de segurança de rede.

A.4 POLÍTICA DE MONITORIZAÇÃO E REGISTO DE EVENTOS

POLÍTICA DE SI	**POL-SI-004.0**
MONITORIZAÇÃO E REGISTO DE EVENTOS	**APROVADO**

Criação 2023-04-26 **Aprovação** 2023-06-19

Introdução

A Empresa Industrial de Borracha (EIB) reconhece a importância da monitorização e registo de eventos como parte integrante das suas medidas de segurança da informação, esta Política estabelece as diretrizes para a monitorização e registo de eventos, visando identificar e responder efetivamente a incidentes de segurança, garantir a conformidade com as políticas e obrigações legais, e proteger os dados pessoais dos indivíduos.

Âmbito

Esta Política abrange a monitorização e registo de eventos em todos os sistemas, infraestrutura e recursos tecnológicos utilizados pela EIB, inclui a implementação de um sistema centralizado de registos (logs), a anonimização dos dados pessoais recolhidos, a sincronização dos relógios entre emissor e servidor, a implementação de um Sistema de Gestão de Eventos e Informações de Segurança (SIEM), e a conformidade com as políticas, procedimentos organizacionais, obrigações legislativas e o Regulamento Geral de Proteção de Dados (RGPD).

Responsabilidades

1. Direção e Gestão
   A direção e a gestão da EIB são responsáveis por:

- Definir e aprovar a política de monitorização e registo de eventos.
- Garantir que os recursos adequados são alocados para a implementação e manutenção de sistemas de monitorização e registo de eventos.
- Promover a conformidade com as políticas, procedimentos organizacionais, obrigações legais e o RGPD.
- Assegurar que a equipa de TI tem o conhecimento e a formação adequados para realizar a monitorização e gestão dos registos de eventos.

2. Departamento de TI

   O Departamento de TI da EIB é responsável por:

   - Implementar e manter um sistema centralizado de registos (logs) que permite o armazenamento e monitorização efetiva dos eventos.
   - Garantir a anonimização adequada dos dados pessoais recolhidos nos registos.
   - Sincronizar os relógios dos emissores com os servidores de registo de eventos.
   - Implementar e gerir um SIEM que permita a análise a correlação de eventos de segurança.
   - Assegurar que a monitorização e gestão dos registos de eventos são realizadas conforme as melhores práticas de segurança da informação.

3. Colaboradores e Utilizadores

   Todos os colaboradores e utilizadores da EIB têm a responsabilidade de:

   - Cumprir com as políticas e procedimentos estabelecidos relativamente à monitorização e registo de eventos.
   - Cooperar com a equipa de TI fornecendo informações relevantes para análise e resposta a incidentes de segurança.
   - Respeitar a privacidade e confidencialidade dos dados pessoais presentes nos registos de eventos.

Diretrizes

1. Armazenamento em Sistema de Registos Centralizado
   Todos os eventos relevantes devem ser registados e armazenados em sistemas centralizados de registos (logs), garantindo a integridade e segurança dos registos.
2. Anonimização dos Dados Pessoais Recolhidos
   Quando forem recolhidos dados pessoais nos registos de eventos, estes devem ser anonimizados de forma a proteger a privacidade dos indivíduos, em conformidade com o RGPD.
3. Sincronização dos Relógios
   É essencial que os relógios dos emissores e servidores de registo de eventos estejam sincronizados para permitir a uma correta correlação dos eventos.
4. Implementação de um SIEM
   Deve ser implementado um SIEM para a análise e correlação de eventos de segurança, permitindo uma identificação mais rápida e eficaz de incidentes e ameaças.
5. Monitorização de Acessos Privilegiados
   Deve-se implementar a monitorização dos acessos privilegiados aos sistemas e recursos da empresa. Registar e analisar as atividades realizadas por utilizadores com privilégios elevados, como administradores de sistemas, com o objetivo de identificar comportamentos suspeitos ou potenciais abusos de privilégios.
6. Monitorização de Tráfego de Rede
   A monitorização do tráfego de rede permite identificar e analisar padrões anómalos, atividades maliciosas ou tentativas de intrusão, deve-se implementar ferramentas de monitorização de tráfego de rede e registar as informações relevantes para uma análise posterior e resposta adequada a incidentes de segurança.
7. Monitorização de Atividades de Utilizadores
   A monitorização das atividades dos utilizadores nos sistemas e aplicações da EIB é importante para detetar comportamentos não autorizados, tentativas de acesso indevido ou atividades suspeitas, devem ser criados registos das atividades dos utilizadores, permitindo a identificação e investigação de eventuais violações de segurança.

8. Monitorização de Integridade de Dados
   É fundamental monitorizar a integridade dos dados armazenados nos sistemas da EIB. Este requisito pode ser realizado mediante técnicas como a comparação de hashes ou assinaturas digitais para verificar se os dados foram alterados de forma não autorizada. Caso seja detetada uma alteração suspeita, deve-se investigar a causa e tomar as medidas necessárias para mitigar o impacto e restaurar a integridade dos dados.

Conclusão

A EIB está comprometida em garantir a monitorização e registo adequados dos eventos de segurança, conforme as políticas, procedimentos organizacionais, obrigações legais e o RGPD. Ao seguir estas diretrizes, a EIB visa proteger a sua infraestrutura, dados pessoais e informações sensíveis, bem como responder efetivamente a incidentes de segurança.

Esta Política de Monitorização e Registos de Eventos será revista periodicamente para garantir a sua eficácia e conformidade com as melhores práticas de segurança da informação e com as alterações legislativas e regulamentares aplicáveis.

A.5 POLÍTICA DE GESTÃO DE ATIVOS

POLÍTICA DE SI **POL-SI-005.0**

GESTÃO DE ATIVOS **APROVADO**

Criação 2023-04-27 **Aprovação** 2023-06-19

Introdução

A política de Gestão de Ativos da Empresa Industrial de Borracha (EIB) estabelece diretrizes para a gestão adequada dos ativos da empresa, incluindo recursos físicos e digitais. A gestão eficaz dos ativos é essencial para garantir a disponibilidade, integridade, confidencialidade e valor dos mesmos, bem como para minimizar riscos e maximizar o retorno do investimento. Esta política define os princípios e responsabilidades para uma gestão de ativos eficiente e consistente em toda a organização.

Âmbito

Esta política aplica-se a todos os funcionários, contratados, fornecedores e outros colaboradores que têm acesso, utilizam ou são responsáveis pela gestão dos ativos da EIB, sejam eles físicos ou digitais e aplica-se a todos os departamentos, unidades de negócio e locais da empresa.

Responsabilidades

1. Direção e Gestão
    - Promover uma cultura de gestão de ativos, estabelecendo prioridades e fornecendo recursos adequados.
    - Designar responsáveis pela implementação e monitorização desta política.

2. Departamento de TI
    - Gerir e supervisionar a infraestrutura tecnológica e os ativos digitais da empresa.
    - Implementar medidas de segurança, como firewalls, antivírus e sistemas de deteção de intrusões, para proteger os ativos digitais.
    - Monitorizar a disponibilidade e o desempenho dos ativos digitais, realizando ações corretivas quando necessário.
    - Manter os sistemas e aplicativos atualizados, garantindo a segurança e a conformidade com as melhores práticas de TI.
    - Realizar testes regulares de backup e recuperação para garantir a integridade e a disponibilidade dos dados.
3. Gestores de Departamento
    - Identificar e classificar os ativos sob a sua responsabilidade.
    - Assegurar a utilização adequada e segura dos ativos.
    - Manter um inventário atualizado dos ativos e garantir a sua integridade.
4. Colaboradores
    - Utilizar os ativos de forma responsável e em conformidade com as políticas e procedimentos estabelecidos.
    - Reportar qualquer perda, roubo ou dano de ativos às pessoas responsáveis.

Diretrizes

1. Inventário de Ativos:
    - Realizar um inventário completo de todos os ativos, incluindo descrição, localização, responsável e outras informações relevantes.
    - Atualizar regularmente o inventário para refletir alterações nos ativos.
2. Classificação dos Ativos:
    - Classificar os ativos de acordo com a sua importância, valor e sensibilidade.

- Definir medidas de proteção adequadas com base na classificação dos ativos.

3. Utilização Responsável dos Ativos:
    - Utilizar os ativos de acordo com as políticas e procedimentos estabelecidos.
    - Evitar a utilização não autorizada, abusiva ou negligente dos ativos.
4. Manutenção e Proteção dos Ativos:
    - Realizar manutenção regular dos ativos para garantir o seu bom funcionamento e prolongar a sua vida útil.
    - Implementar medidas de segurança física e lógica para proteger os ativos contra perdas, danos ou acesso não autorizado.
5. Despromoção de Ativos:
    - Estabelecer procedimentos claros para a despromoção segura e adequada de ativos que não são necessários.
    - Garantir a remoção adequada de informações confidenciais ou sensíveis dos ativos antes da sua despromoção.
6. Atualização Tecnológica:
    - Avaliar regularmente a necessidade de atualização ou substituição de ativos obsoletos, ou com tecnologia ultrapassada.
    - Planear e implementar a atualização dos ativos conforme as necessidades da empresa e as melhores práticas tecnológicas.
7. Controlo de Acesso:
    - Implementar controlos de acesso adequados aos ativos digitais, como autenticação forte, gestão de senhas e privilégios de utilizador.
    - Monitorizar e rever regularmente os direitos de acesso aos ativos digitais para garantir que sejam concedidos apenas aos utilizadores autorizados.
8. Monitorização e Resposta a Incidentes:
    - Implementar sistemas de monitorização de segurança para deteção precoce de incidentes nos ativos digitais.

- Estabelecer procedimentos claros de resposta a incidentes, incluindo a notificação adequada, investigação e mitigação de potenciais violações de segurança.

Conclusão

A política de Gestão de Ativos da EIB estabelece as diretrizes e responsabilidades para a gestão eficaz dos ativos da empresa. Ao seguir esta política, garantimos a proteção adequada dos ativos, a otimização dos recursos e a minimização de riscos associados à sua utilização. Todos os colaboradores são responsáveis por cumprir esta política e contribuir para uma gestão de ativos eficiente e segura.

A.6 POLÍTICA DE ACESSO E CONTROLO DE INFORMAÇÃO

POLÍTICA DE SI **POL-SI-006.0**

ACESSO E CONTROLO DE INFORMAÇÃO **APROVADO**

Criação 2023-04-27 **Aprovação** 2023-06-19

Introdução

A Empresa Industrial de Borracha (EIB) reconhece a importância do acesso e controlo adequado da informação para garantir a confidencialidade, integridade e disponibilidade dos seus recursos de informação. Esta política estabelece diretrizes e responsabilidades para o acesso, utilização e proteção da informação na organização.

Âmbito

Esta política aplica-se a todos os colaboradores, contratados, fornecedores e terceiros que tenham acesso à informação da EIB. Abrange todos os recursos de informação, incluindo sistemas, redes, dados e dispositivos utilizados pela organização.

Responsabilidades

1. Direção e Gestão:
    - Definir e promover uma cultura de segurança da informação na organização.
    - Assegurar a alocação adequada de recursos para implementar e manter medidas de segurança da informação.
    - Nomear responsáveis pela implementação e monitorização das políticas de acesso e controlo de informação.
2. Departamento de TI:

- Gerir e manter os sistemas de informação, incluindo a implementação de controlos de acesso adequados.
- Monitorizar e auditar regularmente os acessos aos recursos de informação para identificar atividades suspeitas ou não autorizadas.

3. Colaboradores e Utilizadores:
   - Cumprir as políticas, procedimentos e diretrizes de acesso e controlo de informação estabelecidos pela EIB.
   - Utilizar apenas os recursos de informação autorizados e conforme responsabilidades profissionais.
   - Proteger as credenciais de acesso, como senhas e tokens de autenticação, e não as partilhar com terceiros.

Diretrizes

1. Autenticação e Autorização:
   - Implementar controlos de autenticação forte para garantir que apenas utilizadores autorizados tenham acesso aos recursos de informação.
   - Conceder privilégios de acesso conforme as responsabilidades e necessidades específicas de cada utilizador.
2. Controlo de Acesso Físico:
   - Limitar o acesso físico a áreas e instalações onde a informação sensível está armazenada ou é processada.
   - Utilizar sistemas de identificação e autenticação adequados para controlar o acesso físico.
3. Controlo de Acesso Lógico:
   - Implementar medidas de controlo de acesso lógico para restringir o acesso aos sistemas e dados somente a utilizadores autorizados.

- Monitorizar e auditar os registos de eventos para detetar atividades suspeitas ou não autorizadas.

4. Classificação da Informação:
   - Classificar a informação conforme a sensibilidade e definir os níveis apropriados de acesso e proteção.
5. Gestão de Contas de Utilizador:
   - Manter um inventário atualizado de contas de utilizador e revogar imediatamente o acesso quando um utilizador deixar a organização ou mudar de função.
   - Implementar políticas de gestão de senhas fortes e exigir alterações regulares de senhas.
6. Educação e Consciencialização em Segurança da Informação:
   - Disponibilizar formação e sensibilização em segurança da informação a todos os colaboradores, contratados e fornecedores.
   - Incentivar a adoção de boas práticas de segurança, tais como a utilização de senhas robustas, a proteção de dispositivos e a identificação de ataques de phishing.
   - Promover a implementação de uma cultura de segurança da informação, incentivando os colaboradores a reportarem incidentes de segurança, partilharem boas práticas e a procurarem constantemente aperfeiçoar os seus conhecimentos e competências na área.
7. Gestão de Dispositivos Móveis:
   - Estabelecer políticas para o uso seguro de dispositivos móveis, como smartphones e tablets, que tenham acesso a recursos de informação da EIB.
   - Exigir a instalação de soluções de segurança, como autenticação multi-fator (MFA) e criptografia, nos dispositivos móveis utilizados para aceder a informações sensíveis.
8. Segregação de Funções:

- Implementar a segregação de funções para garantir que nenhum colaborador tenha privilégios excessivos ou acesso a áreas sensíveis sem necessidade.
- Rever regularmente as atribuições de funções e privilégios de acesso para garantir a conformidade contínua.

Conclusão

A Política de Acesso e Controlo de Informação da EIB estabelece diretrizes claras para garantir que a informação seja acedida e utilizada de forma segura e adequada. Ao seguir estas diretrizes e cumprir as responsabilidades estabelecidas, todos os colaboradores contribuem para a proteção da informação da organização e para a manutenção da sua integridade e confidencialidade.

A.7 POLÍTICA DE SENSIBILIZAÇÃO E FORMAÇÃO EM SI

POLÍTICA DE SI **POL-SI-007.0**

SENSIBILIZAÇÃO E FORMAÇÃO **APROVADO**

Criação 2023-04-27 **Aprovação** 2023-06-19

Introdução

A Empresa Industrial de Borracha (EIB) reconhece a importância da sensibilização e formação em Segurança da Informação (SI) para proteger os seus ativos e garantir a confidencialidade, integridade e disponibilidade das informações. Esta política estabelece diretrizes para promover a consciencialização sobre SI, fornecer formação adequada e realizar simulacros, visando fortalecer a cultura de segurança da informação na organização.

Âmbito

Esta política aplica-se a todos os colaboradores, contratados e fornecedores com acesso a recursos e informações da EIB, independentemente do seu cargo ou função. Todos os envolvidos devem aderir a esta política e participar nas atividades de sensibilização, formação e simulacros em SI.

Responsabilidades

1. A equipa de Recursos Humanos é responsável por coordenar e promover ações de sensibilização, formação e simulacros em SI, em colaboração com o departamento de TI.
2. O departamento de TI é responsável por fornecer formação técnica especializada em SI, manter a infraestrutura de SI atualizada e conduzir os simulacros de incidentes de segurança.

3. A Direção e Gestão deve garantir que os colaboradores participam nas atividades de sensibilização, formação e simulacros em SI, conforme as diretrizes estabelecidas.
4. Os colaboradores são responsáveis por participar ativamente nas atividades de sensibilização, formação e simulacros em SI, aplicar os conhecimentos adquiridos nas suas atividades diárias e relatar quaisquer incidentes de segurança identificados.

Diretrizes

1. Desenvolver um programa abrangente de sensibilização em SI, que inclua comunicações regulares sobre boas práticas, alertas de segurança e consciencialização sobre as ameaças atuais.
2. Realizar ações de formação periódicas em SI, abordando tópicos como proteção de senhas, uso seguro de dispositivos, reconhecimento de phishing e práticas adequadas de partilha de informações.
3. Disponibilizar recursos educativos, como manuais, guias e vídeos, para que os colaboradores se possam informar e atualizar sobre as melhores práticas de SI.
4. Promover a participação em cursos de formação e certificações em SI, fornecendo oportunidades de desenvolvimento profissional nesta área.
5. Realizar simulacros de incidentes de segurança regularmente, com o envolvimento de todos os colaboradores, para testar a resposta da organização a possíveis ameaças e identificar áreas de melhoria.
6. Estabelecer uma cultura de segurança da informação, onde os colaboradores sejam encorajados a relatar incidentes de segurança, partilhar boas práticas e a pesquisar constantemente para aperfeiçoar o conhecimento e competências neste campo.

Conclusão

A EIB está comprometida em promover a sensibilização e formação em SI como parte essencial das suas práticas de segurança. Ao implementar esta política, a organização visa fortalecer a consciencialização sobre SI em todos os níveis, capacitando os colaboradores a

tomar medidas proativas para proteger os ativos e informações da empresa. A realização de simulacros permite testar e aperfeiçoar a resposta da organização a incidentes de segurança.

A.8 POLÍTICA DE DESENVOLVIMENTO DE SOFTWARE

POLÍTICA DE SI **POL-SI-008.0**

DESENVOLVIMENTO DE SOFTWARE **APROVADO**

Criação 2023-04-28 **Aprovação** 2023-06-19

Introdução

A Política de Desenvolvimento de Software define as diretrizes e responsabilidades para o processo de desenvolvimento de software na EIB, esta política visa garantir a criação de software de qualidade, seguro e alinhado com os objetivos estratégicos da empresa e as melhores práticas de desenvolvimento de software.

Âmbito

Esta política aplica-se a todos os funcionários e contratados envolvidos no desenvolvimento de software da EIB, bem como aos fornecedores externos que desenvolvem software em nome da empresa.

Responsabilidades

1. A equipa de desenvolvimento de software é responsável por seguir as melhores práticas, metodologias e padrões estabelecidos, bem como garantir a entrega de software de qualidade.
2. O gestor do projeto é responsável por definir os requisitos do projeto, estabelecer metas realistas, supervisionar o progresso e assegurar a utilização eficiente dos recursos.

3. A equipa de controlo de qualidade é responsável por realizar testes abrangentes, identificar e corrigir falhas, garantindo a conformidade com os requisitos e a qualidade do software desenvolvido.

Diretrizes

1. Práticas de Código Limpo:
   Os programadores devem seguir as melhores práticas de código limpo, escrevendo código legível, modular e bem estruturado. Essas práticas englobam a utilização de nomes de variáveis e funções adequados e representativos, devem evitar a duplicação de código e a aplicar princípios de design sólido.
2. Ambientes Controlados de Testes
   Antes da implantação em ambiente de produção, todos os softwares desenvolvidos devem passar por testes em ambientes controlados. Esses ambientes devem ser configurados para replicar o ambiente de produção de maneira fiel, permitindo a validação e deteção de erros antes do lançamento.
3. Documentação Adequada
   Todo o código desenvolvido deve ser devidamente documentado, fornecendo informações claras sobre a sua finalidade, funcionamento e dependências. A documentação deve ser atualizada sempre que ocorrerem alterações relevantes ao software.
4. Revisões de Código
   O código desenvolvido deve ser submetido a revisões de código por outros membros da equipa. Essa prática permite identificar possíveis erros, garantir a aderência às diretrizes de desenvolvimento e promover a colaboração entre os programadores.
5. Controlo de Versões
   Todo o código-fonte deve ser mantido num sistema de controlo de versões, permitindo o rastreamento de alterações, a reversão para versões anteriores e a colaboração eficiente entre os programadores.

Conclusão

A Política de Desenvolvimento de Software da EIB estabelece as diretrizes e responsabilidades para o desenvolvimento de software interno na organização. Ao aderir a essas diretrizes, a EIB procura garantir a qualidade, segurança e eficiência dos seus próprios produtos de software, promovendo a otimização dos processos internos e o melhor aproveitamento dos recursos tecnológicos. Através da aderência às melhores práticas de desenvolvimento e testes, juntamente com documentação adequada e a gestão eficiente de versões, a EIB visa proporcionar soluções de software confiáveis e de alto desempenho para atender às suas necessidades internas.

A.9 POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO

POLÍTICA DE SI **POL-SI-009.0**

CLASSIFICAÇÃO DA INFORMAÇÃO **APROVADO**

Criação 2023-04-28 **Aprovação** 2023-06-19

Introdução

A política de Classificação da Informação da EIB estabelece diretrizes e responsabilidades para a correta classificação da informação, garantindo a proteção adequada dos ativos de informação da empresa. Esta política visa proteger a confidencialidade, integridade e disponibilidade da informação, bem como facilitar a sua gestão eficaz.

Âmbito

Esta política aplica-se a todos os colaboradores, contratados e terceiros que tenham acesso a informações confidenciais ou sensíveis da EIB, independentemente do formato em que essas informações estejam mantidas.

Responsabilidades

1. Direção e Gestão
   É responsável por estabelecer e rever regularmente as diretrizes de classificação da informação, garantindo que estejam alinhadas com os objetivos de segurança e conformidade da EIB.
2. Gestores de departamentos
   São responsáveis por garantir que os colaboradores sob a sua supervisão estejam cientes das diretrizes de classificação da informação e as sigam corretamente.

3. Colaboradores
   São responsáveis por identificar, classificar e proteger adequadamente as informações confidenciais ou sensíveis com as quais tenham contacto, conforme as diretrizes estabelecidas.

Diretrizes

1. Identificação da Informação
   Os colaboradores devem identificar e marcar claramente as informações conforme a sua confidencialidade, sensibilidade ou valor estratégico. Essa identificação pode ser feita por meio de rótulos, marcas de água ou outros meios apropriados.
2. Classificação da Informação
   A informação deve ser classificada em categorias, como "Confidencial", "Restrito" ou "Público", conforme as diretrizes estabelecidas.
3. Proteção da Informação
   As informações classificadas devem ser protegidas adequadamente, mediante medidas de segurança física e lógica, como controlo de acesso, criptografia e backups regulares.
4. Partilha da Informação
   A Partilha de informações classificadas deve ser restrita apenas às partes autorizadas e conforme os procedimentos estabelecidos.
5. Manuseio e Armazenamento Adequados
   As informações classificadas devem ser manuseadas e armazenadas de forma segura, evitando acesso não autorizado ou divulgação acidental.
6. Retenção e Eliminação
   A retenção e eliminação de informações classificadas devem seguir as políticas e prazos estabelecidos pela EIB e conforme a legislação aplicável.

Conclusão

A Política de Classificação da Informação da EIB é relevante para garantir a proteção adequada das informações e a conformidade com requisitos legais e regulatórios. Todos os colaboradores têm a responsabilidade de seguir as diretrizes estabelecidas e contribuir para a segurança da informação na EIB. A classificação correta da informação é fundamental para a tomada de decisões informadas sobre o tratamento, partilha e proteção da informação.

A.10 POLÍTICA DE GESTÃO E ELIMINAÇÃO DE SUPORTES DE INFORMAÇÃO

POLÍTICA DE SI	**POL-SI-010.0**
GESTÃO E ELIMINAÇÃO DE SUPORTES DE INFORMAÇÃO	**APROVADO**

Criação 2023-04-28 **Aprovação** 2023-06-19

Introdução

A Política de Gestão e Eliminação de Suportes de Informação da EIB estabelece diretrizes e responsabilidades para garantir a adequada gestão, armazenamento e eliminação de suportes físicos e digitais que contenham informações sensíveis ou confidenciais. Esta política visa proteger os ativos de informação da EIB, reduzir o risco de divulgação não autorizada e assegurar a conformidade com as leis e regulamentos aplicáveis.

Âmbito

Esta política abrange todos os suportes de informação utilizados pela EIB, incluindo documentos impressos, CDs, DVDs, unidades de armazenamento externas, discos rígidos, dispositivos USB, cartões de memória, fitas magnéticas, entre outros.

Responsabilidades

1. Direção e Gestão
   É responsável por aprovar e rever periodicamente a política, bem como assegurar a alocação adequada de recursos para sua implementação eficaz.

2. Departamento de SI
   É responsável por supervisionar a implementação da política, garantindo o cumprimento dos requisitos de gestão e eliminação de suportes de informação.
3. Colaboradores
   Todos os colaboradores da EIB devem cumprir esta política, seguindo as diretrizes estabelecidas para a gestão e eliminação adequada de suportes de informação.

Diretrizes

1. Classificação de Informação
   Todos os suportes de informação devem ser devidamente classificados conforme a Política de Classificação da Informação. da EIB, identificando o nível de sensibilidade e confidencialidade.
2. Armazenamento Seguro
   Os suportes de informação devem ser armazenados em locais seguros, protegidos contra acesso não autorizado, danos físicos, incêndios e outros eventos que possam comprometer a sua integridade.
3. Retenção de Informação
   A EIB deve estabelecer políticas claras de retenção de informação, definindo prazos específicos para a manutenção dos suportes conforme as leis e regulamentos aplicáveis. Após o término do prazo, os suportes devem ser adequadamente eliminados.
4. Eliminação Segura
   A eliminação de suportes de informação deve ser realizada de forma segura, garantindo que os dados sejam irrecuperáveis.
5. Registos de Eliminação
   Deve ser mantido um registo de eliminação que documente o processo de eliminação de suportes de informação, incluindo data, tipo de suporte e método de eliminação utilizado.

Conclusão

A Política de Gestão e Eliminação de Suportes de Informação da EIB estabelece diretrizes e responsabilidades para proteger os ativos de informação da empresa. A conformidade com esta política é importante para garantir a confidencialidade, integridade e disponibilidade das informações. Cada colaborador desempenha um papel relevante na aplicação e cumprimento das diretrizes, contribuindo para a segurança geral da EIB.

A.11 POLÍTICA DE CONTROLO CRIPTOGRÁFICO

POLÍTICA DE SI **POL-SI-011.0**

CONTROLO CRIPTOGRÁFICO **APROVADO**

Criação 2023-05-01 **Aprovação** 2023-06-19

Introdução

A Política de Controlo Criptográfico da EIB estabelece diretrizes e requisitos para o uso adequado e seguro de técnicas de criptografia, com o objetivo de proteger a informação confidencial da organização. Esta política visa garantir a confidencialidade, integridade e autenticidade dos dados sensíveis da EIB, bem como o cumprimento das regulamentações aplicáveis relacionadas com a criptografia.

Âmbito

Esta política aplica-se a todos os colaboradores, com acesso aos sistemas e dados da EIB e que utilizam técnicas de criptografia para proteger informações confidenciais.

Responsabilidades

1. Departamento de SI
   É responsável por desenvolver, implementar e monitorizar as práticas de criptografia de acordo com esta política.
2. Colaboradores
   São responsáveis por aplicar as diretrizes de criptografia, utilizar as ferramentas e recursos criptográficos fornecidos pela EIB de maneira adequada e reportar qualquer incidente ou violação de segurança relacionada com criptografia.

Diretrizes

1. Seleção de Algoritmos Criptográficos
   Devem ser utilizados algoritmos criptográficos amplamente reconhecidos e comprovadamente seguros.

   A seleção dos algoritmos deve considerar os requisitos de segurança, interoperabilidade e conformidade regulamentar.

2. Gestão de Chaves Criptográficas
   Deve ser implementado um sistema robusto de gestão de chaves criptográficas, incluindo a geração segura de chaves, distribuição, armazenamento e revogação adequada.

   As chaves criptográficas devem ser protegidas contra acesso não autorizado e mantidas em sigilo.

3. Proteção de Dados Cifrados
   Devem ser implementadas medidas adequadas de proteção dos dados cifrados, garantindo que apenas os destinatários autorizados possam aceder e decifrar as informações.

   Devem ser utilizados protocolos seguros de comunicação para transmitir dados cifrados entre sistemas.

4. Atualização e Manutenção
   Deve ser realizada uma revisão periódica das práticas de criptografia para garantir a conformidade com os padrões atuais e as melhores práticas de segurança.

   Os sistemas e recursos criptográficos devem ser mantidos atualizados com as versões mais recentes de software e correções de segurança.

Conclusão

A Política de Controlo Criptográfico da EIB é fundamental para garantir a proteção eficaz da informação confidencial por meio do uso adequado da criptografia. Ao seguir as

diretrizes estabelecidas nesta política, estaremos a fortalecer a postura de segurança da organização e a proteger os ativos de informação contra ameaças internas e externas.

A adesão a esta política é obrigatória para todos os colaboradores definidos no âmbito e a cooperação e consciencialização de todos é fundamental para garantir a eficácia e o cumprimento dos requisitos de controlo criptográfico.

A.12 POLÍTICA DE CONTROLO DE ACESSOS FISICOS

POLÍTICA DE SI **POL-SI-012.0**

CONTROLO DE ACESSOS FISICOS **APROVADO**

Criação 2023-05-01 **Aprovação** 2023-06-19

Introdução

A política de acesso físico à EIB estabelece diretrizes para garantir a segurança das áreas físicas da organização. Essas medidas visam proteger ativos e informações sensíveis, prevenindo acessos não autorizados e promovendo a integridade, confidencialidade e disponibilidade dos recursos da empresa.

Âmbito

Esta política aplica-se a todos os colaboradores, contratados e visitantes que tenham acesso às instalações físicas da EIB, abrange áreas restritas, salas de servidores, data centers, bastidores, laboratórios e outros espaços sensíveis que contenham ativos e informações críticas.

Responsabilidades

1. Direção e Gestão
   Definir e promover a importância da segurança física nas instalações da EIB.

   Alinhar recursos e orçamentos para garantir a implementação adequada das medidas de segurança física.

2. Departamento de SI
   Elaborar e implementar medidas de segurança física conforme os requisitos legais e regulatórios.

   Monitorizar e auditar regularmente o acesso físico às áreas seguras.

3. Gestores de Departamento
   Assegurar que apenas colaboradores autorizados tenham acesso às áreas restritas conforme com as suas funções.

   Garantir a implementação e conformidade com as diretrizes de segurança física.

Diretrizes

1. Controlo de Acesso
   Utilizar sistemas de identificação e autenticação adequados para controlar o acesso físico.

   Implementar medidas de autenticação forte, como cartões de acesso e códigos PIN.

2. Monitorização e Vigilância
   Instalar e manter sistemas de vigilância, como câmaras de segurança, para monitorizar as áreas seguras.

   Realizar auditorias regulares dos registos de acesso e atividades suspeitas.

3. Gestão de Chaves e Dispositivos de Acesso
   Controlar e auditar o uso de chaves e dispositivos de acesso.

   Manter um registo atualizado de chaves e dispositivos, limitando o acesso a estes recursos.

4. Consciencialização e Treino:
   Realizar formações regulares sobre segurança física, incluindo orientações sobre o manuseio correto de informações e ativos sensíveis.

   Promover a cultura de segurança entre os colaboradores, incentivando a relatar incidentes ou comportamentos suspeitos.

Conclusão

A política de acesso físico à EIB visa garantir a segurança das áreas seguras, protegendo ativos e informações sensíveis, ao seguirmos estas diretrizes e responsabilidades, promovemos um ambiente seguro para o desenvolvimento das atividades da organização e mitigamos potenciais riscos relacionados com o acesso não autorizado. A EIB está comprometida em manter a integridade, confidencialidade e disponibilidade dos seus ativos críticos.

A.13 POLÍTICA DE TRANSFERÊNCIA DE INFORMAÇÃO

POLÍTICA DE SI **POL-SI-013.0**

TRANSFERÊNCIA DE INFORMAÇÃO **APROVADO**

Criação 2023-05-02 **Aprovação** 2023-06-19

Introdução

A presente Política de Transferência de Informação da EIB pretende estabelecer diretrizes e boas práticas para garantir a segurança e a proteção adequada das informações durante o seu processo de transferência entre sistemas, dispositivos e partes interessadas. Esta política visa minimizar os riscos de perda, acesso não autorizado ou divulgação indevida de informações sensíveis durante a transferência.

Âmbito

Esta política aplica-se a todos os colaboradores, contratados e partes interessadas da EIB envolvidos na transferência de informações sensíveis, independentemente do meio utilizado, incluindo transmissões eletrónicas, meios removíveis e comunicações em papel.

Responsabilidades

1. Direção e Gestão
   Fornecer o apoio e os recursos necessários para a implementação efetiva desta política.

   Designar um responsável pela supervisão e gestão das atividades de transferência de informações.

2. Departamento de TI
   Implementar medidas técnicas para garantir a segurança e a integridade das informações durante a transferência.

   Monitorizar e auditar regularmente as atividades de transferência de informações para garantir a conformidade com esta política.

3. Colaboradores e Partes Interessadas
   Cumprir as diretrizes e procedimentos estabelecidos para a transferência de informações.

   Reportar qualquer incidente de segurança ou violação desta política ao responsável designado.

Diretrizes

1. Classificação e Rotulagem:
   Classificar corretamente as informações conforme a sua sensibilidade e aplicar rótulos de segurança correspondentes de acordo com a Política de Classificação da Informação.

   Garantir que apenas informações classificadas para transferência sejam transmitidas e partilhadas.

2. Meios de Transferência
   Utilizar meios de transferência seguros, como redes cifradas ou canais seguros de comunicação.

   Evitar a utilização de meios não seguros ou não autorizados para a transferência de informações sensíveis.

3. Autenticação e Controlo de Acesso
   Utilizar métodos adequados de autenticação e controlo de acesso durante a transferência de informações, como autenticação multi fator (MFA).

4. Encriptação
   Encriptar as informações sensíveis durante a sua transferência, garantindo a confidencialidade e a integridade dos dados.

5. Gestão de Dispositivos de Armazenamento Removíveis
   Controlar e monitorizar o uso de dispositivos de armazenamento removíveis para evitar a transferência não autorizada de informações sensíveis.

Conclusão

A Política de Transferência de Informação da EIB visa proteger a confidencialidade, integridade e disponibilidade das informações durante o seu processo de transferência.

É responsabilidade de todos os colaboradores e partes interessadas cumprir com esta política e adotar as medidas de segurança estabelecidas para garantir a proteção adequada das informações sensíveis. A EIB está empenhada em manter um ambiente seguro para a transferência de informações e irá rever regularmente esta política para garantir a sua eficácia e conformidade contínua com os requisitos de segurança da informação.

A.14 POLÍTICA DE RELAÇÃO COM FORNECEDORES

POLÍTICA DE SI **POL-SI-014.0**

RELAÇÃO COM FORNECEDORES **APROVADO**

Criação 2023-05-02 **Aprovação** 2023-06-19

Introdução

A EIB reconhece a importância da segurança da informação nas relações com os seus fornecedores, esta política estabelece diretrizes e responsabilidades para garantir a proteção adequada das informações partilhadas com os fornecedores, a fim de minimizar os riscos e preservar a confidencialidade, integridade e disponibilidade dos ativos de informação da organização.

Âmbito

Esta política aplica-se a todos os colaboradores, departamentos e fornecedores envolvidos nas relações comerciais com a EIB, abrange todas as informações partilhadas com os fornecedores, independentemente do formato ou meio de transmissão.

Responsabilidades

1. Direção e Gestão
   Definir e promover a importância da segurança da informação nas relações com os fornecedores.

   Designar responsáveis pela implementação e conformidade com esta política.
2. Departamento de Compras
   Incluir cláusulas de segurança da informação nos contratos com os fornecedores.

Avaliar a segurança da informação dos fornecedores antes de estabelecer relações comerciais.

3. Departamento de TI
   Monitorizar e auditar as atividades dos fornecedores em relação à segurança da informação.

   Estabelecer e manter um processo de gestão de riscos relacionados com fornecedores.

Diretrizes

1. Avaliação de Segurança da Informação
   Realizar uma análise de risco dos fornecedores antes de estabelecer relações comerciais.

   Avaliar a adequação das medidas de segurança da informação implementadas pelos fornecedores.

2. Contratos e Acordos
   Incluir cláusulas contratuais que estabeleçam as responsabilidades e obrigações em relação à segurança da informação.

   Especificar requisitos de proteção de informações confidenciais durante o manuseio e armazenamento por parte dos fornecedores.

3. Partilha Controlada de Informações
   Partilhar informações confidenciais com fornecedores apenas quando estritamente necessário.

   Estabelecer mecanismos de controlo e monitorização para garantir o uso apropriado dessas informações.

4. Conformidade com Regulamentos e Normas
   Assegurar que os fornecedores estejam em conformidade com as leis, regulamentos e normas de segurança da informação aplicáveis.

   Incluir requisitos específicos de conformidade nos contratos e monitorizar regularmente a conformidade dos fornecedores.

5. Gestão de Incidentes
   Estabelecer um processo de gestão de incidentes que inclua a notificação e resposta a incidentes de segurança por parte dos fornecedores.

   Coordenar com os fornecedores ações corretivas para remediar incidentes de segurança.

Conclusão

A Política de Segurança da Informação nas relações com os fornecedores da EIB estabelece diretrizes claras e abrangentes para garantir a segurança da informação durante o envolvimento com fornecedores. Ao adotar estas diretrizes, a EIB procura minimizar os riscos e proteger as suas informações sensíveis, promovendo um ambiente seguro e confiável nas suas relações com os fornecedores. É responsabilidade de todos os colaboradores e partes interessadas cumprir e aplicar esta política em todas as interações com fornecedores.

A.15 POLÍTICA DE GESTÃO DE RISCOS

POLÍTICA DE SI **POL-SI-015.0**

GESTÃO DE RISCOS **APROVADO**

Criação 2023-05-12 **Aprovação** 2023-06-19

Introdução

A Empresa Industrial de Borracha (EIB) reconhece a importância crítica da gestão de riscos de segurança da informação para proteger ativos, garantir a confidencialidade, integridade e disponibilidade dos dados e sistemas, e para manter a continuidade dos negócios. Esta política estabelece as diretrizes e responsabilidades para a identificação, avaliação e tratamento de riscos de segurança da informação em toda a organização, conforme os princípios e orientações da norma ISO/IEC 27005.

Âmbito

Esta política aplica-se a todos os colaboradores e parceiros da EIB e abrange todos os processos, atividades, ativos e áreas da organização.

Responsabilidades

1. Direção e Gestão
   Define a estrutura da gestão de riscos e promove a sua implementação eficaz.
   Aloca recursos adequados para a gestão de riscos e garante a conformidade com esta política.
2. Departamento de SI
   Coordena e supervisiona o processo de gestão de riscos em toda a organização.
   Identifica riscos, avalia impactos e a probabilidade, e propõe estratégias de mitigação.

3. Gestores de Departamento
   Identificam riscos específicos relacionados com as suas áreas de influência e aplicam estratégias de gestão adequadas.
   Comunicam riscos relevantes e medidas de mitigação à equipa.
4. Colaboradores
   Reportam os riscos identificados à hierarquia ou ao departamento responsável.

Diretrizes

1. Identificação de Riscos
   Identifica todos os ativos de informação e sistemas críticos para o negócio.
   Identifica e documenta ameaças e vulnerabilidades associadas a cada ativo.
2. Avaliação de Riscos
   Avalia a probabilidade e o impacto de cada risco identificado.
   Classifica os riscos com base em escalas de severidade predefinidas.
3. Tratamento de Riscos
   Desenvolve estratégias de tratamento de riscos, incluindo evitar, reduzir ou mitigar, transferir ou aceitar riscos.
   Implementa medidas de controlo adequadas para mitigar riscos identificados.
4. Monitorização e Revisão
   Monitoriza regularmente o estado dos riscos identificados e a eficácia das medidas de tratamento.
   Realiza revisões periódicas da avaliação de riscos para identificar novas ameaças ou alterações das circunstâncias.
5. Comunicação e Consciencialização
   Comunica os riscos identificados e estratégias de tratamento aos envolvidos.
   Promove a consciencialização sobre a gestão de riscos de segurança da informação em toda a organização.

Conclusão

A EIB está empenhada em manter uma prática sistemática e eficaz para a gestão de riscos de segurança da informação, alinhada com os princípios da norma ISO/IEC 27005. Esta política estabelece as bases para a identificação, avaliação e tratamento de riscos em toda a organização. A colaboração de todos os colaboradores é essencial para garantir que a segurança da informação seja uma prioridade constante e que os riscos sejam tratados de forma apropriada.

B

POLÍTICAS DE USO ACEITÁVEL

B.1 LEIS E NORMAS

POLÍTICA DE USO ACEITÁVEL **POL-UA-001.0**

LEIS E NORMAS **APROVADO**

Criação 2023-05-18 **Aprovação** 2023-06-19

Alcance / Aplicabilidade

Esta política aplica-se a todos os funcionários e colaboradores com acesso a ativos de informação.

Propósito

Esta política exige a definição das leis específicas que os funcionários e colaboradores devem estar cientes.

Política

É necessário que todos os funcionários e colaboradores possuam conhecimento acerca das seguintes leis e normas:

- Lei nº 46/2018;

- Lei n.º 109/2009;
- Lei do RGPD;
- Norma ISO/IEC 27001;
- Norma ISO/IEC 27005;

Manutenção da Política

A equipa de segurança da informação é responsável pela manutenção contínua desta política deve rever a política a cada 5 anos e esta deverá ser atualizada sempre que necessário, a fim de assegurar a relevância e conformidade com as regulamentações em vigor. Qualquer alteração ou revisão da política será comunicada a todos os funcionários e partes interessadas relevantes.

Exceções

Qualquer exceção a esta política deve ser solicitada por escrito e aprovada pela equipa de segurança da informação da EIB. Todas as exceções devem ser documentadas e revistas periodicamente.

Sanções

O não cumprimento desta política pode resultar em medidas disciplinares, incluindo, mas não se limitando a, advertências, suspensões ou rescisões de contrato, conforme as políticas e procedimentos internos da EIB.

B.2 PAPEIS E RESPONSABILIDADES

POLÍTICA DE USO ACEITÁVEL **POL-UA-002.0**

PAPEIS E RESPONSABILIDADES **APROVADO**

Criação 2023-05-18 **Aprovação** 2023-06-19

Alcance / Aplicabilidade

Todos os colaboradores da EIB, incluindo aqueles com atribuições específicas para administração de Sistemas, Base de Dados, Plataformas de Serviços, Equipamentos de Rede dos Sistemas e Tecnologias de Informação e Comunicação, bem como Entidades Externas e Chefias, devem cumprir as diretrizes estabelecidas nesta política.

Propósito

Esta política exige a definição clara dos papéis e responsabilidades dos utilizadores gerais dos recursos de Tecnologia da Informação (TI), assim como dos Administradores de Sistemas, Base de Dados, Plataformas de Serviços e Equipamentos de Rede dos Sistemas de TI e Comunicação.

Responsabilidades

1. Colaboradores e Utilizadores
   Os equipamentos de Tecnologia da Informação (TI) fornecidos pela EIB destinam-se exclusivamente ao exercício das atividades profissionais, devendo ser mantidos em bom estado de conservação e utilizados de forma adequada. Cada utilizador é responsável pela segurança das suas informações pessoais, garantindo que não sejam ilegais, ilícitas ou inadequadas conforme o código de ética da EIB. Os utilizadores

devem cumprir integralmente os termos e condições de utilização do software disponibilizado pela EIB.

2. Administradores de Sistemas, Bases de Dados, Plataformas de Serviço, Equipamentos de Rede dos Sistemas e Tecnologias de Informação e Comunicação

   Um colaborador da EIB, na função de Utilizador, que possua acesso e permissões para administrar sistemas, bases de dados, plataformas de serviço, equipamentos de rede dos sistemas e tecnologias de informação e comunicação, é responsável pela segurança da informação a que tem acesso, bem como pela garantia da confidencialidade dessas informações, conforme Declaração de Confidencialidade obrigado a assinar. A chefia direta tem a responsabilidade de assegurar que apenas os colaboradores que realmente necessitam de acessos privilegiados os possuam, devendo concedê-los, revê-los e remover esses acessos quando deixarem de ser justificados.

   Para além do referido acima, é incumbência dos administradores assegurar que os ativos sob a sua administração técnica estejam conforme esta política. Essa responsabilidade implica no mínimo aplicar as melhores práticas relacionadas à manutenção sustentada da ciber higiene [1] dos referidos ativos, sendo essa uma condição necessária para o cumprimento desta Política.

3. Chefias e quadros intermédios
   Sempre que ocorrer uma mudança nas responsabilidades ou funções de um utilizador interno, é responsabilidade imediata da respetiva chefia informar a área responsável pela gestão de acessos. Isso permite que os privilégios de acesso desse utilizador aos vários recursos de TI sejam revistos e alterados adequadamente. No caso de utilizadores externos, essa responsabilidade passa para o responsável da unidade interna onde o serviço foi contratado.

   Quando um colaborador da EIB deixa de trabalhar para a empresa, DSI deve tomar as seguintes medidas:

   - Desativar todas as contas de acesso, como acesso à Active Directory (AD), acesso a RAS (Remote Access Service) e acesso a VPN;

1 A ciber higiene refere-se às precauções básicas de segurança no ciberespaço. Ao adotar boas práticas de ciber higiene, reduz-se a oportunidade de sucesso de ciberataques

- Revogar os pontos de acesso físico aos edifícios da organização;
- Recolher os cartões de acesso.

No caso de um colaborador externo que, dentro das suas funções, tenha lidado com informação confidencial ou dados pessoais, é necessário destruir todas as informações no seu computador antes de ser reaproveitado por outro utilizador. Estas medidas visam garantir a segurança da informação e proteger a confidencialidade dos dados da empresa.

4. Departamento de Segurança da Informação (DSI)
   É responsável por garantir a conformidade com a presente política, bem como com outras disposições de proteção de dados da União ou dos Estados-Membros, e com as políticas estabelecidas pelo responsável pelo tratamento ou pelo subcontratante em relação à proteção de dados pessoais. Isso inclui a definição de responsabilidades, a sensibilização e formação do pessoal envolvido nas operações de tratamento de dados, e a realização de auditorias correspondentes.

   Também presta aconselhamento, quando solicitado, relativamente à avaliação de impacto sobre a proteção de dados.

Manutenção da Política

O Departamento de Segurança de SI é o responsável pela manutenção, administração e publicação desta política. Deve rever esta política a cada 5 anos e atualizá-la, se necessário, para garantir a sua relevância e conformidade regulatória.

Exceções

Não se aplicam.

Sanções

O Departamento de Segurança de Informação (DSSI) será responsável por identificar eventuais não conformidades com esta política e comunicá-las à administração. Além disso, o DSSI auxiliará a administração no desenvolvimento de um plano de ação corretivo, garantindo que seja implementado num prazo razoável.

B.3 MANUTENÇÃO DE POSTOS E AMBIENTE DE TRABALHO

POLÍTICA DE USO ACEITÁVEL **POL-UA-003.0**

MANUTENÇÃO DE POSTOS E AMBIENTE DE TRABALHO

APROVADO

Criação 2023-05-18 **Aprovação** 2023-06-19

Alcance / Aplicabilidade

Todos os funcionários e colaboradores da EIB

Propósito

Esta política estabelece os procedimentos necessários para se manter o espaço de trabalho conforme as normas da empresa, garantindo que nenhum indivíduo tenha acesso a itens e informações que não lhe pertencem. Promove a manutenção de uma boa limpeza e organização, bem como um ambiente de fácil acesso e leitura.

Política

Os utilizadores têm a responsabilidade de garantir o cumprimento das seguintes medidas:

1. É necessário garantir que os computadores sejam devidamente bloqueados quando não estão a ser utilizados. Deve-se ativar as medidas de segurança adequadas, como a bloqueio de ecrã ou o bloqueio de sessão (Win + L), para impedir o acesso não autorizado às informações e recursos do computador. Esta prática é fundamental para proteger a privacidade dos dados e prevenir possíveis incidentes de segurança.
2. A secretária deve ser mantida limpa, organizada e livre de documentos desnecessários, esta prática contribui para uma fluidez e ambiente de trabalho mais produtivo,

permitindo uma melhor concentração e eficiência. Manter a secretária limpa também evita o risco de informações confidenciais ou sensíveis serem expostas acidentalmente, garantindo a privacidade e a segurança dos dados.

3. Os Utilizadores devem adotar uma prática de "desktop limpo"nos seus computadores, minimizando a quantidade de ícones e arquivos desnecessários na área de trabalho. Esta medida contribui para uma organização mais eficiente, facilita a localização de documentos importantes e promove um ambiente de trabalho mais produtivo.
4. Os utilizadores são responsáveis por garantir que os computadores sejam desligados no final do dia de trabalho, encerrando todos os programas e realizando o encerramento adequado. Esta medida visa garantir a economia de energia e a segurança dos sistemas, além de preservar o bom funcionamento dos equipamentos.
5. É obrigação dos utilizadores remover qualquer informação restrita ou sensível da secretária quando esta não está ocupada e ao final de cada dia de trabalho. Essa informação deve ser devidamente guardada numa gaveta trancada, garantindo assim a sua segurança e confidencialidade. Esta prática visa prevenir o acesso não autorizado a informações sensíveis e assegurar a conformidade com as políticas de segurança da empresa.
6. É obrigatório manter as gavetas que contenham informações restritas ou sensíveis devidamente fechadas e trancadas quando não estão em uso. Essa medida de segurança garante a confidencialidade e proteção dos dados, evitando o acesso não autorizado ou o extravio de informações sensíveis. Ao adotar esta prática, contribuímos para a preservação da privacidade e integridade dos dados, promovendo um ambiente seguro para o tratamento e armazenamento de informações confidenciais.
7. As chaves utilizadas para aceder informações restritas ou sensíveis não devem ser deixadas sem vigilância na secretária. Ao manter as chaves sob vigilância adequada, minimizamos o risco de acesso não autorizado e preservamos a confidencialidade das informações. Recomenda-se que as chaves sejam guardadas em local seguro quando não estiverem em uso, como num cofre, chaveiro ou em posse de uma pessoa autorizada, evitando qualquer possibilidade de perda, roubo ou uso indevido.
8. Dispositivos de computação portáteis, como PCs portáteis e tablets devem ser devidamente trancados utilizando um cabo de segurança ou mantidos numa gaveta

trancada. Esta medida visa garantir a proteção desses dispositivos, que geralmente contêm informações sensíveis e confidenciais. O uso de um cabo de trança permite que o dispositivo seja fisicamente amarrado a um objeto fixo, impedindo o roubo ou remoção não autorizada. Caso não seja possível utilizar um cabo de segurança, é recomendado que o dispositivo seja guardado numa gaveta trancada, garantindo a segurança quando não estiver em uso. Estas práticas contribuem para a proteção dos dados e evitam possíveis incidentes de segurança relacionados ao acesso não autorizado ou perda de equipamentos.

9. É estritamente proibido deixar senhas anotadas em notas adesivas (sticky notes) ou em qualquer lugar acessível, como debaixo do computador, teclado ou em qualquer outra localização facilmente visível ou alcançável. O armazenamento inadequado de senhas representa um risco significativo de segurança, pois pode permitir o acesso não autorizado a sistemas, aplicativos e informações confidenciais. Os utilizadores devem adotar práticas seguras de gestão de senhas, como memorizar as senhas ou utilizar soluções de gestão de senhas seguras. O objetivo é proteger a integridade das informações e evitar potenciais violações de segurança causadas por senhas expostas ou acessíveis a pessoas não autorizadas.

10. Todas as impressões que contenham informações restritas ou sensíveis devem ser recolhidas de imediato da impressora ou fax assim que forem impressas. Os utilizadores devem adotar técnicas de impressão segura ao imprimir documentos que contenham informações restritas ou sensíveis. É fundamental evitar que documentos sensíveis fiquem expostos ou fiquem acessíveis a pessoas não autorizadas. Esta prática ajuda a evitar o acesso não autorizado a informações confidenciais e a proteger a privacidade e a integridade dos dados da empresa.

11. Ao descartar informações ou documentos restritos, ou sensíveis, é essencial que sejam devidamente destruídos para garantir a sua confidencialidade. Recomenda-se o uso de máquinas trituradoras para a destruição física dos documentos. Caso não haja acesso a uma máquina trituradora, os documentos devem ser colocados em caixotes designados para a destruição de informações ou documentos confidenciais. Esses caixotes devem estar devidamente trancados e garantir a proteção adequada durante o transporte e até que a destruição seja realizada de forma segura. É importante seguir as diretrizes e políticas estabelecidas pela empresa em relação ao

descarte de informações confidenciais, a fim de prevenir o acesso não autorizado ou a divulgação indevida desses dados.

12. Quadros que contenham informações restritas ou sensíveis devem ser apagados de forma adequada. Isso significa que qualquer conteúdo confidencial presente nos quadros deve ser removido de forma completa e segura. Recomenda-se o uso de apagadores apropriados para limpar as informações escritas nos quadros. É importante tomar precauções adicionais para garantir que não haja a possibilidade de recuperação das informações apagadas.
13. Os dispositivos de armazenamento em massa, como unidades de CD-ROM, DVD ou USB, devem ser considerados sensíveis devido à possibilidade de conterem informações confidenciais. É crucial que esses dispositivos sejam devidamente protegidos e mantidos em segurança. Recomenda-se que sejam armazenados em gavetas trancadas ou em locais seguros quando não estiverem em uso. Dessa forma, é possível reduzir o risco de perda, roubo ou acesso não autorizado, protegendo assim as informações sensíveis que possam estar armazenadas. É fundamental que os utilizadores adotem medidas adequadas de segurança para proteger esses dispositivos e garantir a confidencialidade das informações neles contida.

Manutenção da Política

O Departamento de Segurança de SI é o responsável pela manutenção, administração e publicação desta política. Deve rever esta política a cada 5 anos e atualizá-la, se necessário, para garantir a sua relevância e conformidade regulatória.

Exceções

Não se aplicam.

Sanções

O Departamento de Segurança de Informação (DSSI) será responsável por identificar eventuais não conformidades com esta política e comunicá-las à administração. Além disso, o DSSI auxiliará a administração no desenvolvimento de um plano de ação corretivo, garantindo que seja implementado num prazo razoável.

B.4 CORREIO ELETRÓNICO EMPRESARIAL

POLÍTICA DE USO ACEITÁVEL **POL-UA-004.0**

CORREIO ELETRÓNICO EMPRESARIAL **APROVADO**

Criação 2023-05-19 **Aprovação** 2023-06-19

Alcance / Aplicabilidade

Todos os funcionários e colaboradores da EIB com acesso a correio eletrónico.

Propósito

A presente política estabelece as diretrizes para o uso apropriado do correio eletrónico empresarial, visando assegurar o cumprimento das normas e procedimentos estabelecidos pela organização.

Política

Todo o uso do correio eletrónico deve ser consistente com as políticas e procedimentos estabelecidos pela EIB, conforme os princípios de conduta e ética, segurança da informação, conformidade legal e boas práticas de negócio aplicáveis. Os colaboradores são responsáveis por seguir as seguintes diretrizes:

1. Uso Profissional
   O correio eletrónico empresarial deve ser utilizado estritamente para fins profissionais relacionados com as atividades da empresa. O uso pessoal do correio eletrónico empresarial deve ser reduzido ao mínimo e restrito a situações devidamente autorizadas.

2. Confidencialidade

   Os colaboradores devem tratar todas as informações recebidas e enviadas por meio do correio eletrónico empresarial como confidenciais e protegê-las de acesso não autorizado. Informações confidenciais não devem ser partilhadas ou divulgadas sem a devida autorização.

3. Uso Adequado

   O correio eletrónico empresarial deve ser utilizado de forma ética, respeitando as leis, regulamentos e políticas internas da empresa. Os colaboradores devem evitar o envio de mensagens ofensivas, difamatórias, discriminatórias, ilegais ou que possam prejudicar a reputação da empresa.

4. Segurança

   É responsabilidade de cada colaborador tomar as devidas precauções para garantir a segurança do correio eletrónico empresarial, isso inclui o uso de senhas fortes, a não partilha de senhas com terceiros, não abrir anexos ou hiperligações suspeitas e relatar imediatamente qualquer atividade suspeita ou violação de segurança.

5. Uso de Recursos

   Os recursos do correio eletrónico empresarial, como armazenamento e largura de banda, devem ser utilizados de forma responsável. O envio em massa de mensagens não relacionadas com trabalho, o encaminhamento de cadeias[2], spam ou qualquer atividade que possa sobrecarregar a infraestrutura de correio eletrónico empresarial são estritamente proibidos.

6. Retenção de Mensagens

   Os colaboradores devem aderir à política de retenção de mensagens da empresa, que determina o período pelo qual as mensagens devem ser mantidas e as diretrizes para a sua exclusão. Entende-se que quatro (4) anos é um período aceitável, podendo o colaborador optar por outro período desde que não coloque em causa o rastreio de atividades profissionais.

7. Monitorização

   A empresa reserva-se ao direito de monitorizar o uso do correio eletrónico empresarial para garantir o cumprimento desta política e para proteger os seus interesses legítimos. Os colaboradores devem estar cientes de que a suas comunicações podem

2 mensagens encaminhadas repetidamente de pedidos de caridade, boa sorte, piadas, entre outros

ser monitorizadas, caso seja necessário, o que não implica que todas as comunicações sejam monitorizadas.

8. Conformidade Legal
   Os colaboradores devem cumprir todas as leis e regulamentos aplicáveis relacionados com o uso do correio eletrónico empresarial, incluindo as leis de proteção de dados e privacidade.

Manutenção da Política

O Departamento de Segurança de SI é o responsável pela manutenção, administração e publicação desta política. Deve rever esta política a cada 5 anos e atualizá-la, se necessário, para garantir a sua relevância e conformidade regulatória.

Exceções

Não se aplicam.

Sanções

O Departamento de Segurança de Informação (DSSI) será responsável por identificar eventuais não conformidades com esta política e comunicá-las à administração. Além disso, o DSSI auxiliará a administração no desenvolvimento de um plano de ação corretivo, garantindo que seja implementado num prazo razoável.

B.5 NAVEGAÇÃO NA INTERNET

POLÍTICA DE USO ACEITÁVEL **POL-UA-005.0**

NAVEGAÇÃO NA INTERNET **APROVADO**

Criação 2023-05-19 **Aprovação** 2023-06-19

Alcance / Aplicabilidade

Todos os funcionários, contratados, estagiários e quaisquer outras pessoas que tenham acesso aos recursos de internet da EIB, seja por meio de dispositivos da empresa ou dispositivos pessoais usados para fins profissionais.

Propósito

Esta política exige a definição do comportamento adequado para garantir uma navegação segura e em conformidade com o código de ética da empresa.

Política

A EIB reconhece a importância da navegação na internet para o desempenho das atividades dos seus colaboradores. No entanto, é fundamental estabelecer diretrizes claras para garantir um uso adequado e responsável dos recursos de internet da empresa. Esta política tem como objetivo estabelecer as diretrizes para a navegação na internet, promovendo a segurança, a produtividade e a conformidade com as leis e regulamentos aplicáveis.

1. Uso adequado
   Os recursos de internet da EIB devem ser usados apenas para fins relacionados com o trabalho. A navegação pessoal não é permitida, exceto quando autorizada pela Direção e Gestão.

2. Uso para fins profissionais
   A navegação na internet deve ser realizada principalmente para fins profissionais e relacionados com as tarefas e responsabilidades dos colaboradores da EIB. É permitido utilizar a internet para pesquisa, comunicação de trabalhos, acesso a recursos relevantes e outras atividades relacionadas com o exercício das funções.
3. Uso consciente do tempo
   A internet pode ser uma ferramenta útil para o trabalho, mas é importante utilizá-la de forma consciente e evitar distrações desnecessárias. Evite navegar em sites não relacionados com o trabalho ou dedicar um tempo excessivo a atividades não produtivas.
4. Segurança da Informação
   Os colaboradores da EIB devem estar cientes dos riscos associados à navegação na internet, como malware, phishing e sites maliciosos, devem tomar as devidas precauções para proteger a segurança da informação, evitando o download de arquivos suspeitos ou visitar sites não confiáveis.
5. Conteúdo adequado
   É proibido o acesso, download ou partilha de conteúdo ofensivo, ilegal, discriminatório, difamatório ou que viole os direitos de autor. Os colaboradores da EIB devem respeitar os princípios de ética e profissionalismo ao utilizar os recursos de internet da empresa.
6. Respeito pelos direitos de autor e propriedade intelectual
   Ao utilizar a internet, é necessário respeitar os direitos de autor e a propriedade intelectual de terceiros, não é permitido copiar, reproduzir ou distribuir material protegido por direitos de autor sem a devida autorização.
7. Redes sociais e fóruns online
   Se o uso das redes sociais for autorizado pela EIB, é importante utilizá-las de forma responsável. Evite publicar informações confidenciais da organização ou de colegas de trabalho, respeite as políticas internas e mantenha uma conduta profissional nas interações online de modo a não prejudicar a imagem da empresa.
8. Respeito pelos outros colaboradores e pela reputação da EIB
   Ao utilizar a internet, é essencial respeitar os direitos e privacidade dos colegas

de trabalho, bem como a reputação e imagem da EIB. Evite publicar conteúdo difamatório, ofensivo ou prejudicial à organização, ou a qualquer outra pessoa.

9. Download de software
   O download de software só é permitido quando autorizado pela equipa de TI. Os colaboradores devem evitar o download de software não autorizado ou que possa comprometer a segurança dos sistemas.

10. Monitorização
    A EIB reserva-se ao direito de monitorizar a navegação na internet dos seus colaboradores para garantir o cumprimento desta política e para proteger a segurança da rede e dos dados da empresa.

11. Educação e consciencialização
    A EIB disponibilizará formações periódicas para consciencializar os seus colaboradores sobre a importância da navegação segura na internet e as consequências do uso inadequado. Os colaboradores da EIB devem participar nessas formações e atualizarem os seus conhecimentos regularmente.

12. Cumprimento das políticas e normas aplicáveis
    Todos os colaboradores devem cumprir as políticas, normas e regulamentos aplicáveis estabelecidos pela EIB, bem como as leis em vigor relacionadas com o uso da internet.

Diretrizes de uso não aceitável

Além das diretrizes já estabelecidas acima é importante destacar algumas práticas consideradas inaceitáveis e estritamente proibidas. O uso não aceitável dos recursos de internet da EIB inclui, mas não se limita a:

1. Acesso a conteúdo ilegal:
   É estritamente proibido aceder, partilhar, transmitir ou descarregar conteúdo ilegal, como material pornográfico de qualquer natureza, conteúdo relacionado com atividades criminosas, incitação ao ódio ou qualquer outro conteúdo que viole as leis e regulamentos em vigor.

2. Assédio ou discriminação
   É proibido utilizar os recursos de internet da EIB para assediar, difamar, discriminar

ou prejudicar outras pessoas com base na sua raça, etnia, religião, género, orientação sexual ou qualquer outra característica protegida pela legislação.

3. Uso inadequado de redes sociais
   É inaceitável o uso de redes sociais para difamar, intimidar, assediar, discriminar ou prejudicar a reputação da EIB, dos seus colaboradores ou de qualquer outra pessoa.

4. Atividades de hacking ou invasão de privacidade
   Qualquer atividade que vise aceder, modificar, danificar ou comprometer os sistemas de informação da EIB, bem como a invasão de privacidade de terceiros, é estritamente proibida.

5. Engenharia social e phishing
   É proibido envolver-se em atividades de engenharia social, phishing ou qualquer ação que vise obter informações confidenciais de terceiros, como senhas, números de cartão de crédito, dados pessoais, etc.

6. Propagação de malware e vírus
   É proibido instalar, distribuir ou propagar qualquer forma de malware, vírus, worms, cavalos de Troia ou qualquer software malicioso que possa comprometer a segurança dos sistemas da EIB.

7. Ativismo
   É proibido utilizar os recursos de internet da EIB para se envolver em atividades de ativismo. Incluindo, mas não se limitando a, promover causas políticas, religiosas ou sociais. Os recursos da EIB devem ser usados exclusivamente para fins relacionados com trabalho e com a missão da organização, evitando a disseminação de informações ou mensagens que possam comprometer a neutralidade ou imparcialidade da instituição.

8. Utilização não autorizada de informações confidenciais
   É inaceitável o uso dos recursos de internet para divulgar, partilhar ou aceder a informações confidenciais da EIB, ou de terceiros sem a devida autorização.

9. Sobrecarga intencional de recursos
   Qualquer ação deliberada que resulte na sobrecarga dos sistemas de rede ou de

servidores, como o envio de spam, a realização de ataques de negação de serviço (DDoS) ou a utilização excessiva da largura de banda, é estritamente proibida.

Manutenção da Política

O Departamento de Segurança de SI é o responsável pela manutenção, administração e publicação desta política. Deve rever esta política a cada 5 anos e atualizá-la, se necessário, para garantir a sua relevância e conformidade regulatória.

Exceções

Não se aplicam.

Sanções

O Departamento de Segurança de Informação (DSSI) será responsável por identificar eventuais não conformidades com esta política e comunicá-las à administração. Além disso, o DSSI auxiliará a administração no desenvolvimento de um plano de ação corretivo, garantindo que seja implementado num prazo razoável.

B.7 ÉTICA E PRIVACIDADE

POLÍTICA DE USO ACEITÁVEL **POL-UA-006.0**

ÉTICA E PRIVACIDADE **APROVADO**

Criação 2023-05-22 **Aprovação** 2023-06-19

Alcance / Aplicabilidade

Todos os colaboradores, contratados, fornecedores e parceiros de negócios da EIB

B.7.0.1 *Propósito*

A EIB compromete-se a conduzir as suas atividades de forma ética, respeitando a privacidade das informações confidenciais e cumprindo as leis e regulamentos de proteção de dados aplicáveis. Esta política tem como objetivo fornecer orientações a todos os envolvidos na EIB, estabelecendo os princípios de conduta ética e as diretrizes para o tratamento adequado das informações confidenciais.

Política

A EIB está empenhada em conduzir as suas atividades de forma ética e em proteger a privacidade das informações confidenciais. A presente política de Ética e Privacidade estabelece diretrizes claras para garantir a integridade, segurança e privacidade das informações confidenciais da EIB e dos seus clientes. Visa estabelecer um ambiente de trabalho ético e responsável, onde a confidencialidade das informações e a proteção da privacidade sejam prioridades essenciais.

1. Confidencialidade das informações
   Os colaboradores da EIB devem manter a confidencialidade das informações confidenciais, incluindo, mas não se limitando a, segredos comerciais, estratégias de negócio, informações financeiras e quaisquer outros dados sensíveis relacionados

com a EIB e com os seus clientes.

As informações confidenciais não devem ser divulgadas a terceiros não autorizados, a menos que expressamente permitido ou exigido por lei.

2. Uso adequado das informações

   As informações confidenciais devem ser utilizadas apenas para fins relacionados com os negócios da EIB e conforme as políticas e procedimentos estabelecidos.

   É proibido o uso das informações confidenciais para benefício pessoal, vantagem competitiva indevida ou qualquer atividade ilegal.

3. Proteção da propriedade intelectual

   A EIB valoriza e protege a sua propriedade intelectual a dos seus clientes e de outros terceiros. Os colaboradores devem respeitar e cumprir os direitos de propriedade intelectual, incluindo patentes, marcas registadas, direitos de autor e segredos comerciais.

4. Segurança da informação

   Os colaboradores devem adotar medidas adequadas de segurança para proteger as informações confidenciais contra acesso não autorizado, uso indevido, perda ou divulgação.

   Devem ser seguidas as diretrizes e os procedimentos estabelecidos pela EIB para garantir a segurança da informação, incluindo o uso de senhas seguras, acesso restrito a sistemas e redes, e a implementação de medidas de proteção contra malware e outras ameaças de segurança.

5. Responsabilidade e conformidade

   Todos os colaboradores são responsáveis por cumprir esta política e as leis de proteção de dados aplicáveis.

   A EIB irá promover a sensibilização e a formação adequada sobre ética e privacidade, visando garantir a consciencialização e a conformidade com as políticas e regulamentos de proteção de dados.

Manutenção da Política

O Departamento de Segurança de SI é o responsável pela manutenção, administração e publicação desta política. Deve rever esta política a cada 5 anos e atualizá-la, se necessário, para garantir a sua relevância e conformidade regulatória.

Exceções

Não se aplicam.

Sanções

O Departamento de Segurança de Informação (DSSI) será responsável por identificar eventuais não conformidades com esta política e comunicá-las à administração. Além disso, o DSSI auxiliará a administração no desenvolvimento de um plano de ação corretivo, garantindo que seja implementado num prazo razoável.

B.8 SOFTWARE E LICENÇAS

POLÍTICA DE USO ACEITÁVEL **POL-UA-007.0**

SOFTWARE E LICENÇAS **APROVADO**

Criação 2023-05-22 **Aprovação** 2023-06-19

Alcance / Aplicabilidade

Esta política aplica-se a todos os colaboradores da EIB que tenham acesso, usem ou distribuam software nas instalações da empresa, ou em dispositivos de propriedade da empresa.

Propósito

O objetivo desta política é garantir o uso adequado de software e respetivas licenças na EIB, promovendo a conformidade legal, a proteção dos direitos de propriedade intelectual e a segurança dos sistemas de informação. A empresa está empenhada em adquirir, instalar, utilizar e manter o software conforme os termos e condições das licenças e contratos estabelecidos pelos fornecedores de software.

Política

A política de Software e Licenças da EIB estabelece diretrizes claras para aquisição, instalação, uso e manutenção de software nas operações da empresa. Ao aderir a esta política, garantimos que o software utilizado seja adequadamente licenciado, respeitando os direitos de propriedade intelectual e assegurando a segurança dos sistemas de informação. A conformidade com esta política é fundamental para manter a integridade e a reputação da EIB no mercado, a seguir apresentam-se a diretrizes para esta política.

1. Aquisição de Software

- Todo o software utilizado na EIB deve ser adquirido legalmente através de fornecedores autorizados ou obtido sob licenças adequadas.
- Antes de adquirir software, deve-se realizar uma análise das necessidades e requisitos, procurando soluções adequadas e licenciadas.

2. Instalação e Uso de Software
    - A instalação de software nos sistemas da EIB deve ser realizada por profissionais autorizados, seguindo os procedimentos estabelecidos pela empresa.
    - O uso de software deve ser estritamente para fins profissionais relacionados com as atividades da empresa.
    - É proibida a instalação, uso ou distribuição de software não licenciado, pirateado, ou que viole os direitos de autor.
3. Atualização e Manutenção de Licenças
    - As licenças de software devem ser regularmente verificadas e atualizadas para garantir a sua validade e conformidade.
    - A renovação de licenças deve ser realizada atempadamente, evitando o uso de software desatualizado ou não licenciado.
4. Uso de Software de Código Aberto (OpenSource)
    - O uso de software de código aberto é permitido na EIB, desde que esteja conforme as licenças de código aberto aplicáveis e que não represente riscos de segurança ou legalidade.
    - O uso de software de código aberto deve ser devidamente documentado e acompanhado de políticas e procedimentos específicos.
5. Auditorias e Conformidade
    - A EIB reserva-se o direito de realizar auditorias internas ou externas para verificar a conformidade com esta política.
    - Qualquer violação desta política pode resultar em ações disciplinares, conforme as políticas e regulamentos internos da empresa.

Manutenção da Política

O Departamento de Segurança de SI em articulação com o departamento de TI é o responsável pela manutenção, administração e publicação desta política. Deve rever esta política a cada 5 anos e atualizá-la, se necessário, para garantir a sua relevância e conformidade regulatória.

Exceções

Não se aplicam.

Sanções

O Departamento de Segurança de Informação (DSSI) será responsável por identificar eventuais não conformidades com esta política e comunicá-las à administração. Além disso, o DSSI auxiliará a administração no desenvolvimento de um plano de ação corretivo, garantindo que seja implementado num prazo razoável.

B.9 TRABALHO REMOTO

POLÍTICA DE USO ACEITÁVEL **POL-UA-008.0**

TRABALHO REMOTO **APROVADO**

Criação 2023-05-23 **Aprovação** 2023-06-19

Alcance / Aplicabilidade

Esta política de Trabalho Remoto aplica-se a todos os colaboradores da EIB, que sejam autorizados a realizar atividades profissionais remotamente.

Propósito

O objetivo desta política é estabelecer diretrizes claras para o trabalho remoto na EIB, assegurando a continuidade das operações, a produtividade e a segurança das informações, além de promover o equilíbrio entre vida profissional e pessoal.

Política

A política de Trabalho Remoto da EIB estabelece diretrizes para a prática do trabalho remoto, garantindo a continuidade das operações da empresa, a produtividade e a segurança das informações. Ao aderir a esta política, tanto a empresa como os colaboradores asseguram que o trabalho remoto seja realizado de forma eficiente, conforme as políticas de segurança e privacidade da EIB. O trabalho remoto proporciona flexibilidade e equilíbrio entre vida profissional e pessoal, promovendo um ambiente de trabalho saudável e produtivo.

1. Autorização para Trabalho Remoto

- O trabalho remoto deve ser autorizado pela gestão, com base na natureza das funções desempenhadas pelo colaborador e nas políticas específicas do departamento.
- A autorização para trabalho remoto é concedida de forma individual, sujeita a revisão e alteração conforme as necessidades da empresa.

2. Condições e Expectativas
    - O colaborador é responsável por estabelecer um ambiente adequado para o trabalho remoto, incluindo uma conexão de internet estável e um local seguro e confortável para realizar as tarefas designadas.
    - O colaborador deve cumprir o horário de trabalho acordado e estar disponível para se comunicar e colaborar com colegas e supervisores, conforme necessário.
3. Acesso Remoto via VPN
    - O acesso aos recursos internos da empresa durante o trabalho remoto deve ser realizado mediante uma conexão VPN segura e devidamente configurada.
    - O colaborador deve seguir as políticas de segurança estabelecidas pela EIB ao utilizar a VPN, incluindo a proteção de informações confidenciais e a não divulgação de credenciais de acesso.
4. Segurança da Informação
    - O colaborador é responsável por garantir a segurança dos dados e informações da empresa durante o trabalho remoto, aderindo às políticas e diretrizes de segurança estabelecidas.
    - O uso de dispositivos pessoais para aceder a sistemas e dados da empresa deve ser realizado com cuidado, seguindo as políticas de segurança da informação e utilizando softwares atualizados e protegidos.
5. Equipamentos e Segurança
    - Os colaboradores devem utilizar os seus próprios computadores pessoais para o trabalho remoto. É responsabilidade dos colaboradores garantir que os seus dispositivos estejam protegidos com soluções de segurança atualizadas, como antivírus e firewall.

- Caso o equipamento utilizado pelos colaboradores não apresente as condições de segurança básicas, a EIB reserva-se ao direito de promover a instalação de aplicativos de segurança necessários para garantir a proteção das informações e a integridade dos sistemas. Em casos extremos, se um equipamento representar um risco significativo para a segurança dos dados da empresa, a EIB poderá recusar a conexão remota desse equipamento.
- Os colaboradores podem solicitar equipamentos à EIB, como portáteis ou outros dispositivos, para desempenhar o trabalho remoto. A requisição dependerá da disponibilidade dos equipamentos.

6. Comunicação e Colaboração
    - Durante o trabalho remoto, o colaborador deve utilizar as ferramentas de comunicação e colaboração designadas pela empresa para se conectar e interagir com colegas e supervisores.
    - A comunicação profissional e respeitosa é fundamental, assim como a partilha adequada de informações e a manutenção da confidencialidade.

Manutenção da Política

O Departamento de Segurança de SI em articulação com o departamento de TI é o responsável pela manutenção, administração e publicação desta política. Deve rever esta política a cada 5 anos e atualizá-la, se necessário, para garantir a sua relevância e conformidade regulatória.

Exceções

Não se aplicam.

Sanções

O Departamento de Segurança de Informação (DSSI) será responsável por identificar eventuais não conformidades com esta política e comunicá-las à administração. Além disso, o DSSI auxiliará a administração no desenvolvimento de um plano de ação corretivo, garantindo que seja implementado num prazo razoável.

B.10 BYOD (BRING YOUR OWN DEVICE)

POLÍTICA DE USO ACEITÁVEL **POL-UA-009.0**

BYOD (BRING YOUR OWN DEVICE) **APROVADO**

Criação 2023-05-23 **Aprovação** 2023-06-19

Alcance / Aplicabilidade

A política de BYOD (Bring Your Own Device) aplica-se a todos os colaboradores da EIB que desejem utilizar os seus próprios dispositivos (como smartphones, tablets, portateis) para fins profissionais.

Propósito

O objetivo desta política é permitir que os colaboradores utilizem os seus dispositivos pessoais para fins profissionais, promovendo a flexibilidade e produtividade no ambiente de trabalho.

Política

A política de BYOD da EIB permite que os colaboradores utilizem os seus próprios dispositivos pessoais para fins profissionais, desde que estejam conforme as diretrizes estabelecidas. Ao adotar esta abordagem, a EIB procura promover a flexibilidade no ambiente de trabalho, permitindo que os colaboradores utilizem dispositivos com os quais já estejam familiarizados. No entanto, é fundamental garantir a segurança e proteção dos dados da empresa, bem como o comprimento das políticas de segurança da informação. Por isso, esta política define diretrizes claras para o registo de dispositivos, segurança dos dispositivos, acesso à rede corporativa e suporte técnico.

1. Registo do Dispositivo

- Todos os dispositivos pessoais que serão utilizados para fins profissionais devem ser registados no departamento de TI da EIB.
- O registo deve incluir informações básicas sobre o dispositivo, como modelo, número de série e informações de contacto do proprietário.

2. Segurança e Proteção de Dados
    - Os colaboradores são responsáveis por garantir que os seus dispositivos estejam protegidos com palavras-passe fortes ou outros métodos de autenticação.
    - Os dispositivos devem possuir soluções de segurança atualizadas, como antivírus e firewall.
    - Os colaboradores devem estar cientes e cumprir as políticas de segurança da informação da EIB, incluindo a proteção de dados confidenciais.
3. Acesso à Rede e Recursos
    - O acesso à rede da empresa e a determinados recursos e sistemas será concedido apenas aos dispositivos pessoais registados.
    - Os colaboradores devem conectar-se à rede corporativa por meio de uma conexão VPN segura.
4. Suporte Técnico
    - O suporte técnico da EIB será fornecido apenas para questões relacionadas com o acesso aos recursos corporativos e à conectividade VPN nos dispositivos pessoais registados.
    - Problemas de hardware ou software dos dispositivos pessoais são da responsabilidade exclusiva do proprietário.

Manutenção da Política

O Departamento de Segurança de SI em articulação com o departamento de TI é o responsável pela manutenção, administração e publicação desta política. Deve rever esta política a cada 5 anos e atualizá-la, se necessário, para garantir a sua relevância e conformidade regulatória.

Exceções

Não se aplicam.

Sanções

O Departamento de Segurança de Informação (DSSI) será responsável por identificar eventuais não conformidades com esta política e comunicá-las à administração. Além disso, o DSSI auxiliará a administração no desenvolvimento de um plano de ação corretivo, garantindo que seja implementado num prazo razoável.

B.11 GESTÃO DE PASSWORDS

POLÍTICA DE USO ACEITÁVEL **POL-UA-010.0**

GESTÃO DE PASSWORDS **APROVADO**

Criação 2023-05-23 **Aprovação** 2023-06-19

Alcance / Aplicabilidade

Esta política aplica-se a todos os colaboradores da EIB que tenham acesso a sistemas, aplicativos e recursos protegidos por palavra-passe.

Propósito

O objetivo desta política é estabelecer diretrizes claras para a criação, uso e proteção de passwords, a fim de garantir a segurança dos sistemas e dados da EIB.

Política

A política de gestão de passwords da EIB visa promover a segurança dos sistemas e dados, estabelecendo diretrizes para a criação, atualização e proteção adequada das passwords. Ao utilizar passwords complexas e atualizá-las regularmente, reduzimos o risco de acesso não autorizado às nossas contas e informações sensíveis. Além disso, a proteção adequada das passwords, evitando a sua partilha e armazenamento inseguro, é fundamental para garantir a confidencialidade dos dados. Recomendamos também a utilização de autenticação de dois fatores sempre que possível, para adicionar uma camada extra de segurança. Através da adoção destas práticas, reforçamos a segurança dos nossos sistemas e contribuímos para proteger a informação da EIB de potenciais ameaças.

1. Complexidade das Passwords

a) As passwords devem ser complexas e incluir uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais.

b) Evite utilizar informações pessoais óbvias, preferências clubistas ou sequências de teclado previsíveis como "123456", "qwerty"ou "abcd1234".

2. Atualização Regular das Passwords
   - As passwords devem ser alteradas regularmente, pelo menos a cada 180 dias;
   - Não utilize a mesma password para vários sistemas ou serviços;
3. Armazenamento e Proteção das Passwords
   - Nunca partilhe a sua password com outras pessoas, incluindo colegas de trabalho;
   - Não anote as passwords em locais acessíveis ou em formato não seguro;
   - Utilize soluções de gestão de passwords seguras, como cofres de passwords ou aplicações de gestão de passwords;
4. Utilização de Autenticação de Dois Fatores (2FA)
   Sempre que possível, ative a autenticação de dois fatores para reforçar a segurança das suas contas. A autenticação de dois fatores requer a introdução de um segundo fator, como um código enviado para o seu smartphone, além da password.
5. Reutilização de Passwords
   Evite reutilizar passwords. Cada nova password deve ser única e não relacionada com as utilizadas anteriormente.

Manutenção da Política

O Departamento de Segurança de SI é o responsável pela manutenção, administração e publicação desta política. Deve rever esta política a cada 5 anos e atualizá-la, se necessário, para garantir a sua relevância e conformidade regulatória.

Exceções

Não se aplicam.

Sanções

O Departamento de Segurança de Informação (DSSI) será responsável por identificar eventuais não conformidades com esta política e comunicá-las à administração. Além disso, o DSSI auxiliará a administração no desenvolvimento de um plano de ação corretivo, garantindo que seja implementado num prazo razoável.

B.12 SEGURANÇA DE DADOS PESSOAIS

POLÍTICA DE USO ACEITÁVEL **POL-UA-011.0**

SEGURANÇA DE DADOS PESSOAIS **APROVADO**

Criação 2023-05-24 **Aprovação** 2023-06-19

Alcance / Aplicabilidade

Esta política aplica-se a todos os funcionários, contratados, subcontratados e terceiros da EIB que lidam com dados pessoais em nome da empresa.

Propósito

O objetivo desta política é estabelecer diretrizes claras e garantir a segurança adequada dos dados pessoais recolhidos, processados e armazenados pela EIB. O cumprimento desta política é fundamental para proteger a privacidade e a confidencialidade dos dados pessoais dos indivíduos e garantir a conformidade com o RGPD.

Política

A EIB reconhece a importância da segurança de dados pessoais e está comprometida em proteger a privacidade dos indivíduos cujos dados são processados pela empresa. Esta política estabelece diretrizes claras para garantir a segurança adequada dos dados pessoais, incluindo a confidencialidade, a minimização de dados, a integridade, a precisão e a segurança dos dados. Todos os funcionários e partes envolvidas devem aderir a esta política e implementar as medidas de segurança adequadas para proteger os dados pessoais. O não cumprimento desta política pode resultar em medidas disciplinares, bem como em responsabilização legal, caso ocorram violações das leis de proteção de dados

aplicáveis, nomeadamente com o RGPD. A EIB adota as seguintes diretrizes para garantir a segurança dos dados pessoais:

1. Classificação e tratamento de dados pessoais
   Os funcionários devem compreender a importância de classificar corretamente os dados pessoais e assegurar o seu tratamento conforme a sua sensibilidade, aconselha-se a utilização de medidas de segurança apropriadas, como a criptografia, sempre que necessário.

2. Confidencialidade e Acesso Controlado
   Os dados pessoais devem ser tratados como informações confidenciais e acedidos apenas por funcionários autorizados que tenham necessidade legítima de acesso.

   Devem ser implementadas medidas de controlo de acesso, como autenticação forte, para proteger os dados pessoais contra acesso não autorizado.

3. Minimização de Dados
   A recolha e o armazenamento de dados pessoais devem ser limitados ao mínimo necessário para a finalidade específica do processamento.

   Os dados pessoais devem ser retidos apenas pelo tempo necessário para cumprir os objetivos do processamento e conforme as obrigações legais aplicáveis.

4. Integridade e Precisão dos Dados
   Devem ser implementadas medidas para garantir a integridade e a precisão dos dados pessoais.

   Atualizações regulares, correções e exclusões devem ser realizadas conforme necessário, e os dados pessoais devem ser mantidos precisos e atualizados.

5. Segurança de Dados
   Devem ser implementadas medidas técnicas e organizacionais apropriadas para proteger os dados pessoais contra perda, acesso não autorizado, divulgação, alteração ou destruição. Incluindo a utilização de firewalls, criptografia, proteção contra malware e atualizações regulares dos sistemas.

6. Monitorização e deteção de violações de segurança
   Deve ser estabelecido um sistema de monitorização contínua para identificar possíveis violações de segurança dos dados pessoais. Isso inclui a implementação de

soluções de deteção de intrusões, registos de auditoria e mecanismos de alerta para notificar prontamente sobre quaisquer incidentes de segurança.

7. Restrição de acesso aos dados pessoais:
   Apenas os funcionários autorizados devem ter acesso aos dados pessoais, seguindo o princípio do "acesso mínimo necessário". É importante implementar controlos de acesso adequados, como autenticação forte e restrições baseadas em funções, para garantir que apenas pessoas autorizadas possam aceder aos dados pessoais.

8. Anonimização dos dados pessoais
   Quando apropriado e permitido pela legislação aplicável, os dados pessoais devem ser anonimizados ou pseudo-anonimizados sempre que possível. A anonimização reduz o risco de identificação dos indivíduos pelos dados e contribui para a proteção da sua privacidade. É importante estabelecer procedimentos e técnicas adequadas para garantir a efetiva e eficaz anonimização dos dados pessoais, seguindo as melhores práticas e as orientações fornecidas pelas autoridades de proteção de dados.

Manutenção da Política

O Departamento de Segurança de SI em articulação com o departamento de RH é o responsável pela manutenção, administração e publicação desta política. Deve rever esta política a cada 5 anos e atualizá-la, se necessário, para garantir a sua relevância e conformidade regulatória.

Exceções

Não se aplicam.

Sanções

O Departamento de Segurança de Informação (DSSI) será responsável por identificar eventuais não conformidades com esta política e comunicá-las à administração. Além

disso, o DSSI auxiliará a administração no desenvolvimento de um plano de ação corretivo, garantindo que seja implementado num prazo razoável.

B.13 INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

POLÍTICA DE USO ACEITÁVEL **POL-UA-012.0**

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO **APROVADO**

Criação 2023-05-24 **Aprovação** 2023-06-19

Alcance / Aplicabilidade

Esta política aplica-se a todos os funcionários, contratados e terceiros que tenham acesso aos sistemas e dados da EIB.

Propósito

O objetivo desta política é estabelecer diretrizes e procedimentos para a notificação, resposta e resolução de incidentes de segurança na EIB. O foco principal é proteger os sistemas, dados e recursos da empresa contra ameaças e minimizar os danos causados por incidentes de segurança.

Política

A política de incidentes de segurança da informação da EIB tem como objetivo estabelecer um processo claro e estruturado para tratar incidentes de segurança da informação. Através dessa política, a EIB visa proteger os seus ativos de informação e minimizar os impactos negativos decorrentes de incidentes de segurança da informação.

Ao seguir esta política, os funcionários e demais partes envolvidas estão comprometidos em reportar prontamente qualquer incidente de segurança ao departamento de segurança da informação da EIB, utilizando o sistema de registo disponível em my.eib.pt. A resposta e

resolução dos incidentes serão tratadas pela equipa de segurança da informação, garantindo ações adequadas para minimizar os danos e prevenir futuras ocorrências.

A política de incidentes de segurança é um componente essencial da estratégia de segurança da informação da EIB, demonstrando o compromisso da empresa em proteger os seus ativos e informações sensíveis. A EIB adota as seguintes diretrizes para tratar incidentes de segurança da informação:

1. Definição de Incidente de Segurança
   Um incidente de segurança é qualquer evento que comprometa a confidencialidade, integridade ou disponibilidade dos sistemas, dados ou recursos da EIB, incluindo, mas não se limitando a, acesso não autorizado, perda ou roubo de dispositivos, malware, tentativas de intrusão e violações de dados pessoais.

2. Notificação de Incidentes
   Todos os incidentes de segurança devem ser notificados imediatamente à equipa de segurança da informação da EIB. A notificação pode ser feita por meio do sistema de registo de incidentes de segurança disponível em my.eib.pt, telefonicamente ou por outros canais designados.

3. Classificação e Avaliação de Incidentes
   Os incidentes de segurança serão classificados e avaliados de acordo com a sua gravidade, potencial impacto e risco para a EIB. Esta classificação permitirá uma resposta adequada e priorizada dos recursos de segurança.

4. Resposta e Resolução de Incidentes
   A equipa de segurança da informação da EIB tomará as medidas necessárias para responder e resolver os incidentes de segurança. Essas medidas podem abranger desde a investigação do incidente até a contenção de danos, recuperação de sistemas afetados e implementação de medidas corretivas para prevenir futuros incidentes.

5. Registo de Incidentes
   Todos os incidentes de segurança devem ser registados no sistema de registo de incidentes disponível em my.eib.pt conforme o procedimento C.2 **PROC-002**. Os detalhes relevantes, como data, hora, descrição do incidente, ações tomadas e resultados, devem ser documentados de forma clara e precisa.

Manutenção da Política

O Departamento de Segurança de SI é o responsável pela manutenção, administração e publicação desta política. Deve rever esta política a cada 5 anos e atualizá-la, se necessário, para garantir a sua relevância e conformidade regulatória.

Exceções

Não se aplicam.

Sanções

O Departamento de Segurança de Informação (DSSI) será responsável por identificar eventuais não conformidades com esta política e comunicá-las à administração. Além disso, o DSSI auxiliará a administração no desenvolvimento de um plano de ação corretivo, garantindo que seja implementado num prazo razoável.

C

PROCEDIMENTOS DE TI

C.1 OPERAÇÕES COM UTILIZADORES

PROCEDIMENTOS DE SI **PROC-001.0**

OPERAÇÕES COM UTILIZADORES **APROVADO**

Criação 2023-06-14 **Aprovação** 2023-07-20

Objetivo

O objetivo deste procedimento é estabelecer diretrizes para o registo de todas as operações relacionadas com a criação, alteração, cancelamento e atribuição de privilégios dos utilizadores. Este procedimento visa garantir a rastreabilidade completa desde o pedido inicial até à conclusão da tarefa, promovendo a transparência e a segurança das operações realizadas.

Âmbito

Este procedimento aplica-se a todos os utilizadores e administradores envolvidos na criação, alteração, cancelamento e atribuição de privilégios dos utilizadores nos ecossistemas da EIB. As operações devem ser registadas no sistema de gestão de tickets disponível em tickets.eib.pt.

Responsabilidades

1. Administradores de sistema
   São responsáveis por executar as operações de criação, alteração, cancelamento e atribuição de privilégios dos utilizadores.
2. Gestores de departamentos
   Devem reportar as necessidades ao departamento de TI, fornecer as informações e aprovações necessárias para as alterações de privilégios dos utilizadores dentro dos seus respetivos departamentos.
3. Utilizadores
   Devem reportar as necessidades de acesso ou alterações de privilégios aos seu gestores.

Procedimentos

1. Pedido de Acesso, Cancelamento ou Alteração de Privilégios
   O utilizador deve submeter um pedido de acesso ou alteração de privilégios para ao seu gestor de departamento.

   O pedido deve conter informações detalhadas, incluindo a justificação, os privilégios solicitados e quaisquer requisitos específicos.

   Por sua vez os gestores de departamento devem encaminhar esses pedidos para o departamento de TI com as devidas correções e a formalizar a necessidade efetiva.
2. Análise e Aprovação do Pedido
   Os administradores de sistema devem analisar o pedido e verificar se a solicitação está conforme as políticas e procedimentos da EIB.

   Caso o pedido seja aprovado, o administrador deve proceder à criação, alteração, cancelamento ou atribuição dos privilégios solicitados.
3. Registo de Operações
   Todas as operações realizadas pelos administradores de sistema devem ser registadas no sistema de gestão de tickets.

O registo deve incluir informações detalhadas sobre as operações realizadas, como a data, a hora, o utilizador afetado e os privilégios atribuídos.

4. Conclusão da Tarefa
   Após a conclusão das operações, o administrador deve comunicar ao utilizador e gestor de departamento o resultado da tarefa realizada. O utilizador por sua vez deve confirmar a satisfação com as alterações efetuadas.

Conclusão

Este procedimento de registo de operações de utilizadores garante a rastreabilidade completa e a transparência das operações relacionadas com a criação, alteração, cancelamento e atribuição de privilégios dos utilizadores no ecossistema aplicacional da EIB. Ao registar todas as etapas do processo no sistema de gestão de tickets, a EIB garante a conformidade com as políticas de segurança da informação e mantém um histórico das operações para fins de auditoria e revisão.

C.2 REGISTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

PROCEDIMENTOS DE SI **PROC-002.0**

REGISTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO **APROVADO**

Criação 2023-06-29 **Aprovação** 2023-07-20

Objetivo

objetivo deste procedimento é estabelecer as diretrizes e responsabilidades para o registo adequado de incidentes de segurança da informação na Empresa de Indústria de Borracha (EIB). O registo detalhado e consistente dos incidentes permitirá uma gestão eficiente e eficaz dos eventos de segurança da informação, possibilitando a análise, resposta e mitigação apropriadas para proteger os ativos de informação da organização.

Âmbito

Este procedimento aplica-se a todos os colaboradores e utilizadores autorizados da EIB, bem como a quaisquer terceiros que possam ter acesso aos sistemas e informações da empresa.

Responsabilidades

1. Departamento de SI
   Responsável pela supervisão e coordenação do processo de registo de incidentes, incluindo a revisão e acompanhamento dos registos.
2. Gestores de Departamento
   Responsáveis por garantir que todos os incidentes de segurança da informação

que ocorram nas suas áreas de responsabilidade sejam devidamente registados e comunicados ao departamento de SI.

3. Colaboradores e Utilizadores Autorizados
   Responsáveis por relatar prontamente quaisquer incidentes de segurança da informação que observem, seguindo os procedimentos estabelecidos.

Procedimentos

1. Registo de Incidentes
   Sempre que um incidente de segurança da informação for detetado ou suspeito, o colaborador ou utilizador deve proceder ao registo imediato na plataforma GLPI em my.eib.pt. Selecione a opção "Forms -> Incidentes de SI" e preencha o formulário com o máximo de detalhes possível. Ao concluir, clique no botão "Enviar"para submeter o relatório.
2. Comunicação e Notificação
   O departamento de SI deve ser notificado logo após o registo do incidente, para poderem iniciar a avaliação e resposta adequada.
3. Análise e Classificação
   O Departamento de SI analisará cada incidente registado para determinar a gravidade e classificação. Incidentes críticos ou de alta gravidade serão tratados como prioritários e receberão atenção imediata.
4. Investigação e Mitigação
   O Departamento de SI conduzirá uma investigação completa de cada incidente, identificando as causas, impacto e eventuais medidas de mitigação para evitar recorrências futuras.
5. Acompanhamento e Resolução
   O Departamento de SI acompanhará o progresso da resolução de cada incidente e garantirá que todas as ações corretivas necessárias sejam implementadas de forma eficaz.

Conclusão

O registo adequado de incidentes de segurança da informação é essencial para a proteção dos ativos da EIB. Através deste procedimento, a organização pode melhorar a capacidade de detetar, responder e prevenir incidentes, minimizando assim o risco de impacto negativo nas operações e reputação. Ao seguir rigorosamente este procedimento e utilizar a plataforma GLPI em my.eib.pt, a EIB reforça o compromisso com a segurança da informação e a proteção dos seus ativos críticos.

ANEXOS

Formulário do GLPI

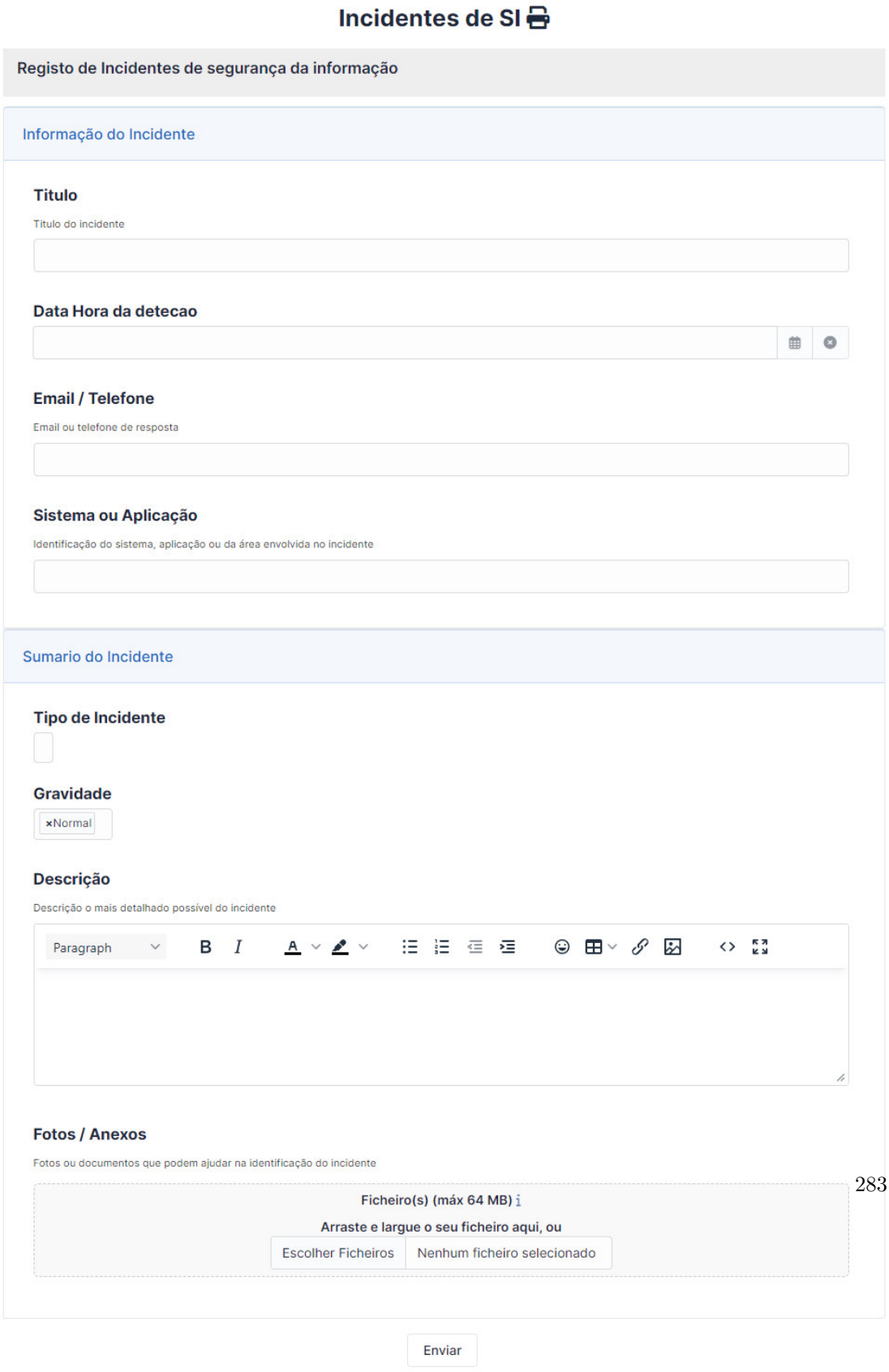


Figura 32: Formulário de Registo de Incidentes de SI no GLPI

D

DECLARAÇÃO DE APLICABILIDADE

Grupo N.Ctrl	Descrição do Controlo	Aplicável (S/N)	Operacionalização - Referência documental Justificação
A.5	**Políticas de segurança da informação**		
A.5.1	**Diretrizes da gestão para a segurança da informação**		
A.5.1.1	Políticas para a segurança da informação	S	A.1 Políticas de SI - Geral B.7 Políticas de uso Aceitável - Ética e Privacidade
A.5.1.2	Revisão das políticas para a segurança da informação	S	6.5 Auditorias internas vertente de SI do Sistema Integrado 6.4 Revisões do Sistema Integrado pela Gestão
A.6	**Organização de segurança da informação**		
A.6.1	**Organização interna**		
A.6.1.1	Papéis e responsabilidades de segurança da informação	S	4.7 Manual de Funções 5.6 Matriz de Riscos de SI
A.6.1.2	Segregação de funções	S	4.7 Manual de Funções 5.6 Matriz de Riscos de SI
A.6.1.3	Contacto com autoridades competentes	S	Contacto com tribunais, PSP e GNR, PJ, CNCS, CNPD no âmbito da prestação de serviços de recuperação de bens, no contexto de processos judiciais
A.6.1.4	Contacto com grupos de interesse especial	S	Contacto com agentes de execução, administradores de insolvência, solicitadores e advogados, no contexto da prestação dos serviços (mencionado nos manuais de procedimentos operacionais)

Continua na próxima página...

Grupo N.Ctrl	Descrição do Controlo	Aplicável (S/N)	Operacionalização - Referência documental Justificação
A.6.1.5	Segurança da informação na gestão de projeto	N	A empresa não desenvolve projetos
A.6.2	**Dispositivos móveis e teletrabalho**		
A.6.2.1	Política de dispositivos móveis	S	B.9 Políticas de uso Aceitável - Trabalho Remoto B.10 Políticas de uso Aceitável - BYOD Termo de Responsabilidade de Telemóvel 5.6 Matriz de Riscos de Segurança da Informação
A.6.2.2	Teletrabalho	S	Políticas de uso aceitável - trabalho remoto
A.7	**Segurança na gestão de recursos humanos**		
A.7.1	**Antes da relação contratual**		
A.7.1.1	Verificação de credenciais e referências	S	CVs de colaboradores e prestadores de serviços Certificados de habilitações e outros documentos comprovativos de competências Entrevista de admissão - Solicitação e validação de referências
A.7.1.2	Termos e condições da relação contratual	S	Contratos de Trabalho Termo de Confidencialidade e de Consentimento de Utilização de Dados Pessoais (Colaboradores) Termo de Confidencialidade para Fornecedores Externos e Prestadores de Serviços
A.7.2	**Durante a relação contratual**		

Continua na próxima página...

Grupo N.Ctrl	Descrição do Controlo	Aplicável (S/N)	Operacionalização - Referência documental Justificação
A.7.2.1	Responsabilidades da gestão	S	Manual do Sistema de Gestão Integrado Código de Conduta Manual de Acolhimento Manual de Funções
A.7.2.2	Consciencialização, educação e formação em segurança da informação	S	Planos de Formação Registos de ações de formação ou similares
A.7.2.3	Procedimento disciplinar	S	Termo de Confidencialidade e de Consentimento de Utilização de Dados Pessoais - Artigo 7º
A.7.3	**Cessação e alteração da relação contratual**		
A.7.3.1	Responsabilidades na cessação ou alteração da relação contratual	S	Manual do Sistema de Gestão Integrado Contratos de Trabalho Termo de Confidencialidade e de Consentimento de Utilização de Dados Pessoais Termo de Confidencialidade e Sigilo para Fornecedores
A.8	**Gestão de ativos**		
A.8.1	**Responsabilidade pelos ativos**		
A.8.1.1	Inventário de ativos	S	5.6 Matriz de Riscos de Segurança da Informação 5.3.4 Inventario de riscos
A.8.1.2	Responsabilidade pelos ativos	S	5.6 Matriz de Riscos de Segurança da Informação 5.3.4 Inventario de riscos
A.8.1.2	Responsabilidade pelos ativos	S	5.6 Matriz de Riscos de Segurança da Informação 5.3.4 Inventario de riscos

Continua na próxima página...

Grupo N.Ctrl	Descrição do Controlo	Aplicável (S/N)	Operacionalização - Referência documental Justificação
A.8.1.3	Utilização aceitável de ativos	S	B.9 Políticas de uso Aceitável - Trabalho Remoto A.10 Políticas de SI - Gestão e eliminação de suportes de informação Termo de Responsabilidade de Telemóvel
A.8.1.4	Devolução de ativos	S	Termo de Responsabilidade de Telemóvel
A.8.2	**Classificação da informação**		
A.8.2.1	Classificação da informação	S	A.9 Política de SI - Classificação da Informação
A.8.2.2	Etiquetagem da informação	S	A.9 Política de SI - Classificação da Informação
A.8.2.3	Manuseamento de ativos	S	B.9 Políticas de uso aceitável - Trabalho remoto A.5 Políticas de SI - Gestão de Ativos A.10 Políticas de SI - Gestão e eliminação de suportes de informação Termo de Responsabilidade de Telemóvel 5.6 Matriz de Riscos de Segurança da Informação
A.8.3	**Manuseamento de suportes de dados**		
A.8.3.1	Gestão de suportes de dados amovíveis	S	A.10 Políticas de SI - Gestão e eliminação de suportes de informação
A.8.3.2	Eliminação de suportes de dados	S	A.10 Políticas de SI - Gestão e eliminação de suportes de informação
A.8.3.3	Transporte de suportes de dados	S	A.10 Políticas de SI - Gestão e eliminação de suportes de informação
A.9	**Controlo de acesso**		
A.9.1	**Requisitos de negócio para controlo de acesso**		
A.9.1.1	Política de controlo de acesso	S	A.6 Políticas de SI - Acesso e controlo de Informação
A.9.1.2	Acesso a redes e a serviços de rede	S	A.6 Políticas de SI - Acesso e controlo de Informação
A.9.2	**Gestão de acesso de utilizadores**		

Continua na próxima página...

Grupo N.Ctrl	Descrição do Controlo	Aplicável (S/N)	Operacionalização - Referência documental Justificação
A.9.2.1	Registo e cancelamento de utilizador	S	A.6 Políticas de SI - Acesso e controlo de Informação C.1 Procedimentos - Operações com Utilizadores Segmentação de grupos por perfil de utilizador
A.9.2.2	Disponibilização de acesso aos utilizadores	S	A.6 Políticas de SI - Acesso e controlo de Informação C.1 Procedimentos - Operações com Utilizadores Segmentação de grupos por perfil de utilizador
A.9.2.3	Gestão de direitos de acesso privilegiado	S	A.6 Políticas de SI - Acesso e controlo de Informação C.1 Procedimentos - Operações com Utilizadores Segmentação de grupos por perfil de utilizador
A.9.2.4	Gestão da informação secreta para autenticação de utilizadores	S	A.6 Políticas de SI - Acesso e controlo de Informação C.1 Procedimentos - Operações com Utilizadores Segmentação de grupos por perfil de utilizador
A.9.2.5	Revisão de direitos de acesso de utilizadores	S	A.6 Políticas de SI - Acesso e controlo de Informação C.1 Procedimentos - Operações com Utilizadores Segmentação de grupos por perfil de utilizador
A.9.2.6	Remoção ou ajuste de direitos de acesso	S	A.6 Políticas de SI - Acesso e controlo de Informação C.1 Procedimentos - Operações com Utilizadores Segmentação de grupos por perfil de utilizador
A.9.3	**Responsabilidades dos utilizadores**		
A.9.3.1	Utilização da informação secreta para autenticação	S	A.6 Políticas de SI - Acesso e Controlo de Informação A.11 Políticas de SI - Controlo Criptográfico B.3 Políticas de uso aceitável - Manutenção de posto e Ambiente de Trabalho

Continua na próxima página...

Grupo N.Ctrl	Descrição do Controlo	Aplicável (S/N)	Operacionalização - Referência documental Justificação
A.9.4	**Controlo de acesso a sistemas e aplicações**		
A.9.4.1	Restrição de acesso à informação	S	A.6 Políticas de SI - Acesso e Controlo de Informação
A.9.4.2	Procedimentos seguros de início de sessão	S	A.6 Políticas de SI - Acesso e Controlo de Informação
A.9.4.3	Sistema de gestão de senhas	S	A.6 Políticas de SI - Acesso e Controlo de Informação
A.9.4.4	Utilização de programas utilitários privilegiados	S	A.6 Políticas de SI - Acesso e Controlo de Informação
A.9.4.5	Controlo de acesso ao código fonte de programas	S	A.6 Políticas de SI - Acesso e Controlo de Informação A.8 Políticas de SI - Desenvolvimento de Software
A.10	**Criptografia**		
A.10.1	**Controlos criptográficos**		
A.10.1.1	Política sobre a utilização de controlos criptográficos	S	A.11 Políticas de SI - Controlo Criptográfico
A.10.1.2	Gestão de chaves	S	A.11 Políticas de SI - Controlo Criptográfico
A.11	**Segurança física e ambiental**		
A.11.1	**Áreas seguras**		
A.11.1.1	Perímetro de segurança física	S	A.12 Políticas de SI - Controlo de Acessos Físicos
A.11.1.2	Controlos de entrada física	S	A.12 Políticas de SI - Controlo de Acessos Físicos
A.11.1.3	Segurança em escritórios, salas e instalações	S	A.12 Políticas de SI - Controlo de Acessos Físicos
A.11.1.4	Proteção contra ameaças externas e ambientais	S	A.12 Políticas de SI - Controlo de Acessos Físicos
A.11.1.5	Trabalhar em áreas seguras	S	A.12 Políticas de SI - Controlo de Acessos Físicos
A.11.1.6	Áreas de carga e descarga	S	A.12 Políticas de SI - Controlo de Acessos Físicos
A.11.2	**Equipamento**		

Continua na próxima página...

Grupo N.Ctrl	Descrição do Controlo	Aplicável (S/N)	Operacionalização - Referência documental Justificação
A.11.2.1	Colocação e proteção de equipamentos	S	Equipamentos instalados de forma a reduzir os riscos de ameaças e perigos ambientais e oportunidades de acesso não autorizado, conforme as políticas em vigor na empresa
A.11.2.2	Serviços básicos de suporte	S	Utilização de UPS's para alimentação de equipamentos críticos
A.11.2.3	Segurança de cablagem	S	Utilização de cablagem elétrica de acordo com os regulamentos aplicáveis Cablagem de rede separada da cablagem elétrica Remoção e instalação completa em 2019
A.11.2.2	Serviços básicos de suporte	S	Utilização de UPS's para alimentação de equipamentos críticos
A.11.2.3	Segurança de cablagem	S	Utilização de cablagem elétrica de acordo com os regulamentos aplicáveis Cablagem de rede separada da cablagem elétrica, remoção e instalação completa em 2019.
A.11.2.4	Manutenção de equipamentos	S	Equipamentos mantidos de acordo com o planeado
A.11.2.5	Remoção de ativos	S	A.5 Políticas de SI - Gestão de Ativos 5.6 Matriz de Riscos de Segurança de Informação
A.11.2.6	Segurança de equipamentos e ativos fora das instalações	S	A.5 Políticas de SI - Gestão de Ativos 5.6 Matriz de Riscos de Segurança de Informação
A.11.2.7	Eliminação e reutilização seguras de equipamentos	S	A.10 Políticas de SI - gestão e eliminação de suportes de informação
A.11.2.8	Equipamento de utilizador não vigiado	S	B.3 Políticas de uso aceitável - Manutenção de postos e ambiente de trabalho
A.11.2.9	Política de secretária limpa e écran limpo	S	B.3 Políticas de uso aceitável - Manutenção de postos e ambiente de trabalho
A.12	**Segurança de operações**		
A.12.1	**Procedimentos e responsabilidades operacionais**		

Continua na próxima página...

Grupo N.Ctrl	Descrição do Controlo	Aplicável (S/N)	Operacionalização - Referência documental Justificação
A.12.1.1	Procedimentos de operação documentados	S	Manuais e Helps das aplicações Documentos internos de apoio
A.12.1.2	Gestão de alterações	S	Alterações ao SGI, aos processos, recursos ou sistemas, planeadas e geridas através do planeamento do SGI
A.12.1.3	Gestão da capacidade	S	Plano de Capacidade e Continuidade
A.12.1.4	Separação entre ambientes de desenvolvimento, teste e de produção	S	A.8 Políticas de SI - Desenvolvimentos de Software
A.12.2	**Proteção contra código malicioso**		
A.12.2.1	Controlos contra código malicioso	S	Firewall e Endpoints
A.12.3	**Salvaguarda de dados**		
A.12.3.1	Salvaguarda de informação	S	A.2 Políticas de SI - Backups e recuperação
A.12.4	**Registos de eventos e monitorização**		
A.12.4.1	Registos de eventos	S	A.4 Políticas de SI - Motorização e registo de eventos Logs de atividades de sistemas, redes e aplicações
A.12.4.2	Proteção da informação registada	S	A.4 Políticas de SI - Motorização e registo de eventos
A.12.4.3	Registos de administrador e de operador	S	A.4 Políticas de SI - Motorização e registo de eventos Logs de atividades de sistemas, redes e aplicações
A.12.4.4	Sincronização de relógio	S	A.4 Políticas de SI - Motorização e registo de eventos Sincronização automática através do Sistema Operativo, no servidor e postos de trabalho locais
A.12.5	**Controlo de software em sistemas de produção**		

Continua na próxima página...

Grupo N.Ctrl	Descrição do Controlo	Aplicável (S/N)	Operacionalização - Referência documental Justificação
A.12.5.1	Instalação de software nos sistemas de produção	S	A.6 Políticas de SI - Acesso e controlo de informação
A.12.6	**Gestão de vulnerabilidades técnicas**		
A.12.6.1	Gestão de vulnerabilidades técnicas	S	B.8 Políticas de uso aceitável - Software e Licenças
A.12.6.2	Restrições sobre a instalação de software	S	B.8 Políticas de uso aceitável - Software e Licenças
A.12.7	**Considerações para auditorias a sistemas de informação**		
A.12.7.1	Controlos de auditoria nos sistemas de informação	S	A.4 Políticas de SI - Motorização e registo de eventos
A.13	**Segurança de comunicações**		
A.13.1	**Gestão de segurança da rede**		
A.13.1.1	Controlos da rede	S	A.3 Políticas de SI - Redes Arquitetura de rede
A.13.1.2	Segurança de serviços de rede	S	A.3 Políticas de SI - Redes Contrato de assistência técnica com prestadores de serviços Termo de Confidencialidade e Sigilo para Fornecedores
A.13.1.3	Segregação das redes	S	A.3 Políticas de SI - Redes Arquitetura de rede
A.13.2	**Transferência de informação**		
A.13.2.1	Políticas e procedimentos de transferência de informação	S	A.13 Políticas de SI - Transferência de informação
A.13.2.2	Acordos sobre transferência de informação	S	Contrato de assistência técnica com prestador de serviços Termo de Confidencialidade e Sigilo para Fornecedores

Continua na próxima página...

Grupo N.Ctrl	Descrição do Controlo	Aplicável (S/N)	Operacionalização - Referência documental Justificação
A.13.2.3	Mensagens eletrónicas	S	A.13 Políticas de SI - Transferência de informação Utilização de canais seguros
A.13.2.4	Acordos de confidencialidade ou de não divulgação	S	Contratos de Trabalho Código de Conduta Manual de Acolhimento Termo de Confidencialidade e Sigilo para Fornecedores
A.14	**Aquisição, desenvolvimento e manutenção de sistemas**		
A.14.1	**Requisitos de segurança de sistemas de informação**		
A.14.1.1	Especificação e análise de requisitos de segurança da informação	S	Políticas de SI
A.14.1.2	Proteger serviços aplicacionais nas redes públicas	S	Políticas de SI
A.14.1.3	Proteger transações de serviços aplicacionais	S	A.13 Políticas de SI - Transferência de informação
A.14.2	**Segurança no desenvolvimento e nos processos de suporte**		
A.14.2.1	Política de desenvolvimento seguro	S	A.8 Políticas de SI - Desenvolvimento de software
A.14.2.2	Procedimentos de controlo de alterações aos sistemas	S	Alterações aos sistemas planeadas e geridas através do planeamento do SGI
A.14.2.3	Revisão técnica de aplicações após alterações na plataforma de produção	S	Alterações aos sistemas planeadas e geridas através do planeamento do SGI Testes de validação antes da entrada em produção
A.14.2.4	Restrições sobre alterações em pacotes de software	S	A.8 Políticas de SI - Desenvolvimento de software Software de terceiros a empresa não tem acesso ao código-fonte
A.14.2.5	Princípios de engenharia de sistemas seguros	S	A.8 Políticas de SI - Desenvolvimento de software
A.14.2.6	Ambiente de desenvolvimento seguro	S	A.8 Políticas de SI - Desenvolvimento de software

Continua na próxima página...

Grupo N.Ctrl	Descrição do Controlo	Aplicável (S/N)	Operacionalização - Referência documental Justificação
A.14.2.7	Desenvolvimento subcontratado	N	A empresa não recorre à subcontratação para o desenvolvimento de aplicações ou sistemas de informação
A.14.2.8	Testes de segurança de sistemas	S	A.8 Políticas de SI - Desenvolvimento de software
A.14.2.9	Testes de aceitação de sistemas	S	A alteração de qualquer sistema obriga a realização de testes de funcionamento antes da sua entrada em produção
A.14.3	**Dados de teste**		
A.14.3.1	Proteção de dados de teste	S	A.8 Políticas de SI - Desenvolvimento de software
A.15	**Relações com fornecedores**		
A.15.1	**Segurança da informação nas relações com os fornecedores**		
A.15.1.1	Política de segurança da informação para as relações com fornecedores	S	A.14 Políticas de SI - Relação com fornecedores A.13 Políticas de SI - Transferência de informação Termo de Confidencialidade para Fornecedores e Prestadores de Serviços 5.6 Matriz de Riscos de Segurança da Informação
A.15.1.2	Endereçar a segurança nos acordos com os fornecedores	S	A.14 Políticas de SI - Relação com fornecedores A.13 Políticas de SI - Transferência de informação Contratos com fornecedores e prestadores de serviços Termo de Confidencialidade para Fornecedores e Prestadores de Serviços 5.6 Matriz de Riscos de Segurança da Informação

Continua na próxima página...

Grupo N.Ctrl	Descrição do Controlo	Aplicável (S/N)	Operacionalização - Referência documental Justificação
A.15.1.3	Cadeia de fornecimento de tecnologias de informação e comunicação	S	A.14 Políticas de SI - Relação com fornecedores A.13 Políticas de SI - Transferência de informação Contratos com fornecedores e prestadores de serviços Termo de Confidencialidade para Fornecedores e Prestadores de Serviços 5.6 Matriz de Riscos de Segurança da Informação
A.15.2	**Gestão da entrega de serviços pelos fornecedores**		
A.15.2.1	Monitorizar e rever serviços de fornecedores	S	A.14 Políticas de SI - Relação com fornecedores Avaliação de fornecedores
A.15.2.2	Gerir alterações aos serviços de fornecedores	S	A.14 Políticas de SI - Relação com fornecedores Contratos com fornecedores e prestadores de serviços Termo de Confidencialidade para Fornecedores e Prestadores de Serviços
A.16	**Gestão de incidentes de segurança da informação**		
A.16.1	**Gestão de incidentes de segurança de informação e melhorias**		
A.16.1.1	Responsabilidades e procedimentos	S	B.13 Políticas de Uso Aceitavel - Incidentes de Segurança da Informação Não Conformidades e Ações de Melhoria Registo de Ocorrências / Plano de Ações
A.16.1.2	Reportar eventos de segurança da informação	S	B.13 Políticas de Uso Aceitavel - Incidentes de Segurança da Informação Não Conformidades e Ações de Melhoria Registo de Ocorrências / Plano de Ações
A.16.1.3	Reportar pontos fracos de segurança da informação	S	B.13 Políticas de Uso Aceitavel - Incidentes de Segurança da Informação Não Conformidades e Ações de Melhoria Registo de Ocorrências / Plano de Ações

Continua na próxima página...

Grupo N.Ctrl	Descrição do Controlo	Aplicável (S/N)	Operacionalização - Referência documental Justificação
A.16.1.4	Avaliação e decisão sobre eventos de segurança da informação	S	B.13 Políticas de Uso Aceitavel - Incidentes de Segurança da Informação Não Conformidades e Ações de Melhoria Registo de Ocorrências / Plano de Ações
A.16.1.5	Resposta a incidentes de segurança da informação	S	B.13 Políticas de Uso Aceitavel - Incidentes de Segurança da Informação Não Conformidades e Ações de Melhoria Registo de Ocorrências / Plano de Ações
A.16.1.6	Aprender com os incidentes de segurança da informação	S	B.13 Políticas de Uso Aceitavel - Incidentes de Segurança da Informação Não Conformidades e Ações de Melhoria Registo de Ocorrências / Plano de Ações
A.16.1.7	Recolha de evidências	S	B.13 Políticas de Uso Aceitavel - Incidentes de Segurança da Informação Não Conformidades e Ações de Melhoria Registo de Ocorrências / Plano de Ações
A.17	**Aspetos de segurança da informação na gestão da continuidade do negócioo**		
A.17.1	**Continuidade de segurança da informação**		
A.17.1.1	Planeamento da continuidade de segurança da informação	S	Plano de Capacidade e Continuidade (A Implementar)
A.17.1.2	Implementação da continuidade de segurança da informação	S	Plano de Capacidade e Continuidade (A Implementar)
A.17.1.3	Verificar, rever e avaliar a continuidade de segurança da informação	S	Plano de Capacidade e Continuidade (A Implementar) 6 - Monitorização, Avaliação, Comunicação e Melhoria contínua
A.17.2	**Redundâncias**		

Continua na próxima página...

Grupo N.Ctrl	Descrição do Controlo	Aplicável (S/N)	Operacionalização - Referência documental Justificação
A.17.2.1	Disponibilidade dos recursos de processamento da informação	S	Plano de Capacidade e Continuidade (A Implementar)
A.18	**Conformidade**		
A.18.1	**Conformidade com requisitos legais e contratuais**		
A.18.1.1	Identificação da legislação aplicável e de requisitos contratuais	S	B.1 Politica uso Aceitavel - Leis e Normas Avaliação da Conformidade Legal - Segurança da Informação Contratos com clientes, fornecedores, colaboradores, prestadores de serviços ou outras partes interessadas
A.18.1.2	Direitos de propriedade intelectual	S	B.8 Politica uso Aceitavel - Software e Licenças 5.6 Matriz de Riscos de Segurança da Informação
A.18.1.3	Proteção de registos	S	A.2 Políticas de SI - Backup e Recuperação Controlo de Informação Documentada Políticas e permissões de acesso implementadas nos sistemas e aplicações
A.18.1.4	Privacidade e proteção de dados pessoais	S	A.9 Políticas de SI - Classificação da Informação B.12 Politica uso Aceitavel - Segurança de Dados Pessoais Avaliação da Conformidade Legal - Segurança da Informação
A.18.1.5	Regulamentação de controlos criptográficos	S	A.11 Políticas de SI - Controlo Criptográfico Avaliação da Conformidade Legal - Segurança da Informação
A.18.2	**Revisões de segurança da informação**		

Continua na próxima página...

Grupo N.Ctrl	Descrição do Controlo	Aplicável (S/N)	Operacionalização - Referência documental Justificação
A.18.2.1	Revisão independente de segurança da informação	S	Auditorias Programa de auditorias ao Sistema Integrado 6.5 Auditorias internas à vertente de Segurança da Informação do Sistema Integrado (Entidades externas) 6.5 Auditorias externas à vertente de Segurança da Informação do Sistema Integrado
A.18.2.2	Conformidade com as políticas e normas de segurança	S	Auditorias 6.5 Auditorias internas à vertente de Segurança da Informação do Sistema Integrado Revisões do Sistema Integrado pela Gestão
A.18.2.3	Revisão da conformidade técnica	S	Auditorias 6.5 Auditorias internas à vertente de Segurança da Informação do Sistema Integrado

E

AUDITORIA DE DIAGNÓSTICO

4A Consultores, Lda

Auditoria de Diagnóstico

Sistema de Gestão de Segurança de Informação

: ***EIB – Empresa Industrial de Borracha, SA***

Auditoria de Diagnóstico – Sistemas de Gestão de Segurança de Informação

CLIENTE: EIB – Empresa Industrial de Borracha, SA

DATA: 30e 31/03/2023

1. Normas de Referência

- ISO/ IEC 27001:2022

2. Equipa Auditora

NOME	FUNÇÃO	ASSINATURA
Rui Ralha Antunes	Coordenador	(Relatório enviado por e-mail)
Nuno Brás	Auditor	(Relatório enviado por e-mail)

3. Locais Auditados

- Sede / Fábrica da Empresa – Marinha Grande

4. Lista de Pessoas contactadas em Auditoria (Nome - Função)

- Tiago [redacted] – Diretor Geral
- Sérgio Lavos – IT Manager
- Isabel [redacted] – Responsável de RH
- Sónia [redacted] – Diretora de Qualidade e Ambiente
- Fernanda [redacted] – Técnica de Segurança
- Catarina [redacted] – Técnica de Segurança

5. Resumo da Auditoria

A presente auditoria de diagnóstico teve como objetivo avaliar o cumprimento dos requisitos da Norma ISO 27001:2022, pela EIB, de modo a permitir à organização definir, planear e implementar ações de melhoria com vista a uma possível futura certificação da Empresa pelo referido referencial.

No decorrer da presente auditoria de diagnóstico foram analisadas às práticas e a documentação existente e verificadas as condições de acesso físico e lógico, bem como as condições "ambientais" para garantir um adequado controlo operacional da segurança de informação.

Foram evidenciadas algumas práticas que se encontram desde já adequadas face ao referencial normativo, no entanto, o Sistema necessita de grande evolução em termos da respetiva documentação e de consolidação de práticas.

Na presente auditoria de diagnóstico foram identificadas 26 não conformidades.

De salientar que, para além da resolução das constatações enumeradas, para a obtenção da certificação, será igualmente necessária a realização de uma auditoria interna e da Revisão pela Gestão.

Como pontos fortes destacam-se:

- Condições do Datacenter (exceto acessos); e
- Boas práticas de escrita de código em termos de modularidade e comentários

A Equipa Auditoria agradece a forma cordial e franca como foi recebida e acompanhada durante o decorrer da presente Auditoria, facto que contribuiu muito positivamente para o desenrolar da mesma.

6. Descrição de Não Conformidades

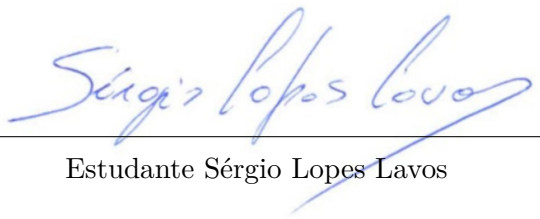
Nº	ISO/IEC 27001:2022		Descrição
	Requisitos	Controlos	
1	4.1	-	A Análise SWOT (versão de 2021) é omissa em vários aspetos relevantes associados à segurança da informação. Exemplos: conhecimentos dos Colaboradores em matérias de cibersegurança, adequabilidade dos ativos informáticos
2	4.2	-	A Empresa identificou as Partes Interessadas e respetivos requisitos, no entanto não inclui algumas relevantes para o SGSI. Exemplos: Entidade Reguladoras (exemplo: CNPD) e requisitos das Partes Interessadas de SI (Exemplo: Clientes – Confidencialidade)
3	4.2	A. 5.31	Não há evidência da identificação dos requisitos legais relevantes para a Segurança da Informação nem da abordagem ao seu cumprimento. Nota: A EIB tem uma metodologia implementada para a identificação de requisitos legais para a Qualidade e Ambiente
4	5.2	A..5.1	Não foi elaborada a Política de Segurança de Informação.
5	5.3	A.5.2	Não estão definidas Funções e responsabilidades dos Colaboradores, bem como os respetivos em termos de SI
6	6.1.1	-	Não estão identificados os Riscos e Oportunidades de Segurança de Informação
7	6.1.3	-	Inexistência de uma declaração de aplicabilidade
8	6.2	-	Não estão definidos Objetivos de Segurança de Informação
9	7.2	A.6.3	Não estão previstas / não foram realizadas (2022 e 2023) ações de formação de SI
10	7.5.3	A5.10 / A.5.34	No que concerne ao controlo de Documentação "Confidencial" em suporte de papel, foram identificadas as seguintes situações: - candidatura do IAPMEI numa sala de reuniões / sala de café; - Sala de reuniões "Exterior" com armários não fechados ou com chave no trinco com dados pessoais – justificação de faltas – 2020/ 2021 e vencimentos 2019 / 2020 - FAT em armário aberto, na Sala de RH
11	8.1	A.5.10	As Regras e procedimentos para uso aceitável de ativos não estão documentadas
12	8.1	A.5.15	O Sistema de controlo de acessos não tem restrições horárias, nem existe prática de revisão periódica dos mesmos.
13	8.1	A.5.18	Não está formalizado o processo de saída de Colaboradores no que concerne à desativação / eliminação dos acessos lógicos (AD, VPN, etc.) e dos acessos físicos (sistema de controlo de acessos)
14	8.1	A.5.18	Não está formalizado o processo de alteração de funções dos Colaboradores no que concerne à alteração dos acessos lógicos
15	8.1	A.5.26	Inexistência de procedimento documentado para resposta a incidentes de Segurança da Informação
16	8.1	A.5.29	Não há evidências de planeamento e testes de respostas destinadas a garantir a continuidade da segurança da informação em caso de disrupção
17	8.1	A.5.34	CCTV – zonas sem sinalética ou sinalética nas duas possíveis entradas do exterior (está apenas na principal)
18	8.1	A.5.34	Algumas câmaras do Sistema de CCTV filmam espaço público e propriedades vizinhas
19	8.1	A.5.34	Sistema de armazenamento das imagens de CCTV num bastidor cuja chave está no fecho, numa sala sem controlo de acessos
20	8.1	A.7.1	Sala de servidores sem acesso restrito
21	8.1	A.7.7	Não está implementada a regra de secretária limpa e ecrã limpo, foram detetadas situações de várias pastas e documentos de trabalho no ambiente

			de trabalho dos Colaboradores
22	8.1	A.7.10	Verificada a existência de Computadores velhos e / ou avariados sem que o disco tenha sido destruído ou formatado
23	8.1	A.8.1	Não existe a prática de bloquear os PC's quando os Colaboradores de ausentam do Posto de Trabalho. Nota: está parametrizado o bloqueio após 30' de não utilização
24	8.1	A.8.9	Gestão de configurações não é feita de modo formal nem se encontra documentada
25	8.1	A.8.25	Não há evidência de realização de testes de segurança durante o ciclo de vida do desenvolvimento
26	8.1	A.8.27	Não há evidência da aplicação, de forma sistemática, de princípios de engenharia de sistemas seguros no desenvolvimento nem da sua documentação. Nota: foram observadas boas práticas implementadas na escrita modular de código e na inclusão de comentários no mesmo

D E C L A R A Ç Ã O

Declaro, sob compromisso de honra, que o trabalho apresentado nesta dissertação, com o título *"Implementação de um Sistema de Gestão de Segurança de Informação (SGSI) baseado na norma ISO/IEC 27001 na EIB,SA"*, é original e foi realizado por Estudante Sérgio Lopes Lavos (2200343) sob orientação de Professor Doutor Leonel Filipe Simões Santos
(leonel.santos@ipleiria.pt).

Leiria, Setembro de 2023



Estudante Sérgio Lopes Lavos