MARCELO SOUSA UEHARA

DIAGNÓSTICO DE CONFORMIDADE DE SEGURANÇA DA INFORMAÇÃO COM AS NORMAS ISO/IEC 27001 E ISO/IEC 27002 EM UMA EMPRESA FINANCEIRA DE SERVIÇOS DIGITAIS

Trabalho de formatura apresentado à Escola Politécnica da Universidade de São Paulo para a obtenção do diploma de Engenharia de Produção.

São Paulo

2024

MARCELO SOUSA UEHARA

DIAGNÓSTICO DE CONFORMIDADE DE SEGURANÇA DA INFORMAÇÃO COM AS NORMAS ISO/IEC 27001 E ISO/IEC 27002 EM UMA EMPRESA FINANCEIRA DE SERVIÇOS DIGITAIS

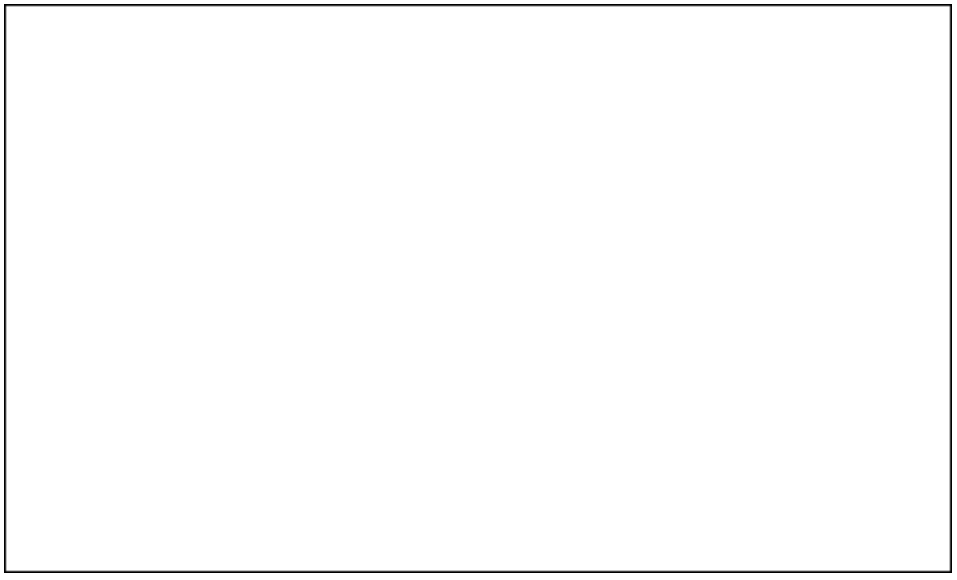
Trabalho de formatura apresentado à Escola Politécnica da Universidade de São Paulo para a obtenção do diploma de Engenharia de Produção.

Orientador: Professor Doutor Fernando Tobal Berssaneti

São Paulo

2024

FICHA CATALOGRÁFICA



DIAGNÓSTICO DE CONFORMIDADE DE SEGURANÇA DA INFORMAÇÃO COM AS NORMAS ISO/IEC 27001 E ISO/IEC 27002 EM UMA EMPRESA FINANCEIRA DE SERVIÇOS DIGITAIS

Marcelo Sousa Uehara

Trabalho de formatura apresentado à Escola Politécnica da Universidade de São Paulo para a obtenção do diploma de Engenharia de Produção.

Aprovado em: _____/_____/_____.

BANCA EXAMINADORA

_____

Orientador

[Nome do Professor Orientador]

[Instituição do membro da banca]

_____

Membro da banca (1)

[Nome do membro da banca]

[Instituição do membro da banca]

_____

Membro da banca (2)

[Nome do membro da banca]

[Instituição do membro da banca]

AGRADECIMENTOS

A Deus, por me conceder força, sabedoria e perseverança ao longo de todo este processo.

Ao meu orientador, por propor o tema deste trabalho e por sua orientação valiosa. Seus conhecimentos e sua experiência foram fundamentais para o desenvolvimento e aprimoramento deste projeto.

Aos demais professores que de alguma forma contribuíram significativamente para este trabalho, expresso minha gratidão também.

À minha mãe, meu pai, minha irmã e toda a minha família, cuja compreensão, paciência e apoio incondicional foram essenciais para que eu pudesse seguir em frente, mesmo nos momentos mais desafiadores.

À minha namorada, por seu amor, incentivo e constante presença ao meu lado, proporcionando-me motivação e conforto ao longo dessa jornada.

Aos meus amigos, por todo o suporte e companheirismo, e por acreditarem em mim e no meu potencial. Suas palavras de encorajamento e apoio foram de grande importância.

Finalmente, agradeço a todos que, de alguma forma, contribuíram para a realização deste trabalho, seja através de conversas, sugestões ou simplesmente estando presentes. Este trabalho é resultado de um esforço coletivo, e sou extremamente grato a cada um de vocês.

RESUMO

Na era digital, as ameaças à segurança da informação têm aumentado consideravelmente, impactando diretamente as operações, reputação e a saúde financeira das organizações. Em 2024, o Brasil registrou 4,7 mil incidentes cibernéticos, refletindo um aumento de 135% em relação ao ano anterior, o que ressalta a urgência de medidas de segurança mais robustas. Este trabalho tem como objetivo avaliar a conformidade dos controles de segurança da informação de uma empresa de serviços financeiros com as normas ISO/IEC 27001 e ISO/IEC 27002. Para tanto, foi realizado um estudo de caso que envolveu a coleta de dados internos por meio de entrevistas com funcionários-chave e análise de documentos, além de dados externos provenientes de relatórios públicos.

Os resultados obtidos indicam que a empresa apresenta 89% de conformidade com as normas ISO/IEC 27001 e ISO/IEC 27002, com boas práticas implementadas em áreas como políticas de segurança, controle de acesso, criptografia e proteção contra *malware*. Contudo, áreas como gestão da segurança na cadeia de suprimentos de Tecnologia da Informação e Comunicação (TIC), gestão de ativos e inventário de informações são algumas das lacunas significativas. A análise também revelou que, embora o time de Segurança da Informação tenha uma visão mais positiva sobre as capacidades da empresa em comparação com outras unidades de negócios, ainda existem desafios para alcançar uma conformidade total.

Com base nesses achados, o estudo propõe um plano de ação para melhorar as áreas deficientes, focando na documentação de processos, treinamento contínuo, aprimoramento dos controles de segurança e maior integração entre os times. Com as melhorias recomendadas, a empresa estará mais preparada para mitigar riscos, fortalecer a proteção de seus ativos digitais e alcançar a conformidade de 100% com as normas ISO/IEC, garantindo a continuidade dos negócios em um cenário de crescente ameaça digital.

Palavras-chave: Segurança da Informação, ISO/IEC 27001, ISO/IEC 27002, Cibersegurança, Estrutura NIST, Gestão de Riscos.

ABSTRACT

In the digital age, threats to information security have increased considerably, directly impacting organizations' operations, reputation and financial health. In 2024, Brazil recorded 4,700 cyber incidents, reflecting an increase of 135% over the previous year, which underscores the urgency of more robust security measures. This work aims to assess the compliance of a financial services company's information security controls with the ISO/IEC 27001 and ISO/IEC 27002 standards. To this end, a case study was carried out involving the collection of internal data through interviews with key employees and document analysis, as well as external data from public reports.

The results obtained indicate that the company has 89% compliance with the ISO/IEC 27001 and ISO/IEC 27002 standards, with good practices implemented in areas such as security policies, access control, encryption and malware protection. However, areas such as security management in the Information and Communication Technology (ICT) supply chain, asset management and information inventory are some of the significant gaps. The analysis also revealed that although the Information Security team has a more positive view of the company's capabilities compared to other business units, there are still challenges to achieving full compliance.

Based on these findings, the study proposes an action plan to improve deficient areas, focusing on process documentation, continuous training, improved security controls and greater integration between teams. With the recommended improvements, the company will be better prepared to mitigate cyber risks, strengthen the protection of its digital assets and achieve 100% compliance with ISO/IEC standards, guaranteeing business continuity in a scenario of growing digital threats.

Keywords: Information Security, ISO/IEC 27001, ISO/IEC 27002, Cybersecurity, Framework NIST, Risk Management.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE SIGLAS

5W+1H	*What, Why, When, Who, Where, How*
AC	*Identity Management and Access Control*
AE	*Anomalies and Events*
AM	*Asset Management*
AN	*Analysis*
AT	*Awareness and Training*
BE	*Business Environment*
BUs	*Business Units*
CM	*Security Continuous Monitoring*
CO	*Communications*
CPR	*Check Point Research*
CSF	*Cybersecurity Framework*
DDoS	*Distributed Denial of Service*
DE	*Detect*
DP	*Detection Processes*
DS	*Data Security*
ICT	*Information and Communication Technology*
ID	*Identify*
IEC	*International Electrotechnical Commission*
IIP	Identificação de Informação e Procedimentos
IM	*Improvements*
InfoSec	*Information Security*
IP	*Information Protection Processes and Procedures*
ISO	*International Organization for Standardization*
GV	*Governance*
MA	*Maintenance*
MI	*Mitigation*
NBR	Norma Brasileira
NIST	*National Institute of Standards and Technology*
NTP	*Network Time Protocol*
PDF	*Portable Document Format*
PR	*Protect*

PT	*Protective Technology*
RA	*Risk Assessment*
RC	*Recover*
RM	*Risk Management Strategy*
RP	*Recovery Planning*
RP	*Response Planning*
RS	*Respond*
SC	*Supply Chain Risk Management*
SGSI	Sistema de Gestão da Segurança da Informação
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
VPNs	*Virtual Private Networks*

SUMÁRIO

1. INTRODUÇÃO

Este tópico irá abordar a introdução do trabalho, fornecendo uma visão geral sobre o contexto do tema, os objetivos, a justificativa e como está estruturado neste trabalho.

1.1. Contextualização do Tema

Na era digital, as organizações enfrentam um número crescente de ameaças à segurança da informação que podem ter consequências graves para as suas operações, reputação e bem-estar financeiro. Consequentemente, a gestão eficaz da segurança da informação tornou-se um requisito essencial para as empresas de vários setores, incluindo o setor fianceiro.

No segundo trimestre de 2024, a *Check Point Research* (CPR) reportou um aumento significativo de aproximadamente 30% nos ataques cibernéticos globais (1.636), em comparação com o mesmo período do ano anterior (1.258). Esse crescimento foi impulsionado por diversos fatores, incluindo a transformação digital contínua, a sofisticação crescente dos cibercriminosos utilizando técnicas avançadas como inteligência artificial e aprendizado de máquina, e a motivação econômica por trás de ataques como *ransomware* e *phishing*. Setores como Educação e Pesquisa foram os mais visados, registrando uma média de 3.341 ataques por semana, seguidos pelos setores Governamental/Militar e Saúde, com 2.084 e 1.999 ataques semanais por organização, respectivamente. As regiões mais afetadas foram a África, com uma média de 2.960 ataques semanais por organização, e a América Latina, que viu um aumento de 53% nos ataques cibernéticos em relação ao ano anterior, alcançando 2.667 ataques semanais (CHECK POINT RESEARCH, 2024).

Recentemente, o governo brasileiro registrou um aumento significativo nos incidentes cibernéticos. No primeiro semestre de 2024, foram reportados 4,7 mil incidentes cibernéticos, um aumento substancial em comparação aos 2 mil incidentes registrados no mesmo período do ano anterior. Este aumento de 135% reflete uma preocupação crescente com a segurança digital e a necessidade de medidas mais robustas para proteger informações sensíveis e sistemas críticos. O número de vazamentos de dados também apresentou um crescimento alarmante. Entre 2020 e 2023, foram notificadas 1,6 mil ocorrências de vazamento de dados, enquanto apenas na metade de 2024 esse número já atingiu 3,2 mil. Este cenário ressalta a

urgência de fortalecer as estratégias de segurança da informação para mitigar os riscos associados a ataques cibernéticos e proteger as infraestruturas digitais do governo e das empresas (GLOBO, 2024).

Os setores mais atingidos por ataques hackers são os serviços financeiros, governos e serviços públicos. Essas áreas têm sido particularmente visadas devido ao valor e à sensibilidade das informações que manejam, tornando-as alvos atrativos para cibercriminosos (CORREIO BRAZILIENSE, 2024).

Uma das estruturas mais amplamente reconhecidas para a gestão da segurança da informação são as normas ISO/IEC 27001 e ISO/IEC 27002. Estas normas internacionais fornecem um conjunto abrangente de diretrizes e melhores práticas para estabelecer, implementar e manter um sistema de gestão da segurança da informação numa organização (JAKÁBOVÁ ET AL., 2013).

A norma ISO/IEC 27001 especifica os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI), enquanto a norma ISO/IEC 27002 fornece um código de práticas para os controles de segurança da informação. Em conjunto, estas normas oferecem um quadro sólido para as organizações avaliarem os seus riscos de segurança da informação, implementarem controles adequados e garantirem a conformidade e a melhoria contínua (ISO/IEC 27001:2022; ISO/IEC 27002:2022).

No contexto de uma empresa no setor financeiro que oferece serviços digitais, a adoção e implementação das normas ISO/IEC 27001 e ISO/IEC 27002 pode proporcionar vários benefícios. Em primeiro lugar, pode ajudar a organização a identificar e gerir os riscos específicos de segurança da informação associados às suas ofertas de serviços digitais, tais como violações de dados, acesso não autorizado e interrupções de serviços. Em segundo lugar, pode ajudar a garantir a confidencialidade, integridade e disponibilidade dos ativos de informação críticos da empresa, que são essenciais para manter a confiança dos clientes e a continuidade operacional (DISTERER, 2013; ROY, 2020).

Além disso, a conformidade com as normas ISO/IEC 27001 e ISO/IEC 27002 pode melhorar a reputação e a credibilidade da empresa no mercado, tornando-a mais atrativa para potenciais clientes e parceiros que valorizam práticas robustas de segurança da informação (ROY, 2020; JAKÁBOVÁ ET AL., 2013; ACHMADI ET AL., 2018; DISTERER, 2013).

Para diagnosticar o nível de conformidade da segurança da informação numa empresa que oferece serviços digitais, deve ser realizado um processo de avaliação abrangente. Este pode envolver a revisão das políticas, procedimentos e controles de segurança da informação

existentes na organização, bem como a realização de avaliações de risco, análises de vulnerabilidades e entrevistas a funcionários para identificar eventuais lacunas ou áreas a melhorar (DISTERER, 2013; ACHMADI ET AL., 2018).

Ao alinharem-se com os requisitos das normas ISO/IEC 27001 e ISO/IEC 27002, as empresas que oferecem serviços digitais podem reforçar a sua postura de segurança da informação, mitigar os riscos e demonstrar o seu empenho em proteger os dados dos seus clientes e garantir a integridade das suas ofertas digitais (DISTERER, 2013; JAKÁBOVÁ ET AL., 2013).

1.2. Objetivo

O objetivo deste trabalho é realizar um diagnóstico abrangente sobre a segurança da informação em uma empresa que atua no setor financeiro e que oferece serviços digitais. Este diagnóstico buscará avaliar o nível de conformidade da empresa com as normas ISO/IEC 27001 e ISO/IEC 27002, identificar lacunas e propor melhorias para fortalecer a postura de segurança da informação da organização. Para atingir esse objetivo, serão adotados os seguintes passos:

I. Revisão de Políticas e Procedimentos: Análise das políticas, procedimentos e controles de segurança da informação atualmente implementados na empresa (situação atual da companhia), comparando-os com os requisitos das normas ISO/IEC 27001 e ISO/IEC 27002.
II. Entrevistas com Funcionários: Condução de entrevistas com funcionários de diferentes níveis e departamentos para compreender a percepção e a implementação das práticas de segurança da informação na organização.
III. Identificação de Lacunas: Comparação dos achados da avaliação com as melhores práticas e diretrizes das normas ISO/IEC 27001 e ISO/IEC 27002, identificando lacunas e áreas que necessitam de melhorias.
IV. Propostas de Melhoria: Desenvolvimento de recomendações e um plano de ação para abordar as lacunas identificadas, melhorar a segurança da informação e assegurar a conformidade contínua com as normas ISO/IEC 27001 e ISO/IEC 27002.

Este diagnóstico permitirá à empresa fortalecer suas práticas de segurança da informação, mitigar riscos associados a ataques cibernéticos e demonstrar seu compromisso com a proteção dos dados dos clientes e a integridade das suas ofertas digitais.

1.3. Justificativa

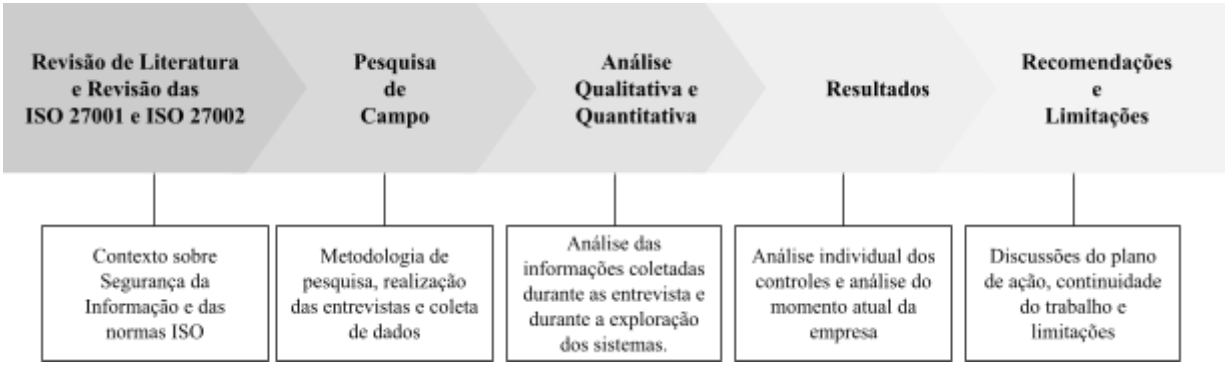
A realização deste trabalho é justificada pela crescente preocupação com a segurança da informação no contexto digital atual, mencionado anteriormente, onde as empresas enfrentam ameaças cibernéticas em constante evolução. O aumento significativo de incidentes cibernéticos, como evidenciado pelos dados recentes, ressalta a urgência de fortalecer as estratégias de cibersegurança.

Além disso, a conformidade com as normas ISO/IEC 27001 e ISO/IEC 27002 não apenas ajuda a proteger dados sensíveis, mas também melhora a reputação da empresa, atrai clientes e garante a continuidade operacional. Portanto, este diagnóstico é crucial para identificar áreas de melhoria e assegurar que a organização esteja adequadamente preparada para enfrentar os desafios de segurança da informação.

1.4. Estrutura do Trabalho

Este trabalho está dividido em 5 partes: Revisão da Literatura, Pesquisa de Campo, Análise (Qualitativa e Quantitativa), Resultados, Recomendações e Limitações Para ilustrar melhor, a figura 1 abaixo oferece uma visão geral de cada etapa estruturada deste trabalho.

Figura 1: Estrutura de Pesquisa



Fonte: Autoria própria

2. FUNDAMENTAÇÃO TEÓRICA

Este tópico abordará uma perspectiva teórica sobre os temas discutidos ao longo do trabalho, bem como as referências utilizadas.

2.1. Conceitos de Gestão de Riscos

A gestão do risco é uma componente crítico do sucesso organizacional, abrangendo a identificação, avaliação e mitigação de potenciais ameaças e incertezas, trazendo benefícios em seus processos, garantindo a qualidade deles (Rampini & Berssaneti, 2024). Gestão de risco é o processo de identificação, avaliação e priorização de riscos, seguido pela aplicação de recursos para minimizar, monitorar e controlar a probabilidade e o impacto de eventos adversos. Essa abordagem permite que organizações antecipem e respondam a ameaças, garantindo a continuidade dos negócios e a proteção de ativos, informações e reputação. A gestão eficaz de riscos contribui para a tomada de decisões informadas e para o alcance de objetivos estratégicos (Assi, 2021).

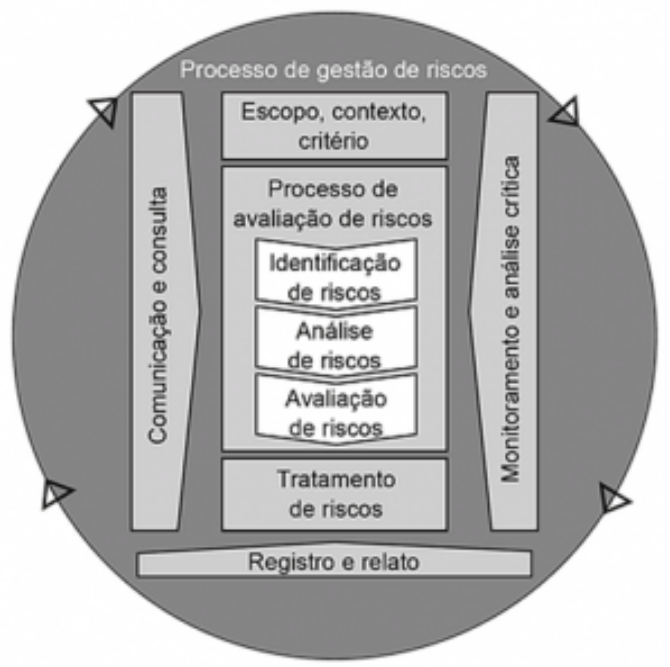
A literatura destaca a correlação entre práticas sólidas de gestão do risco e o desempenho do projeto. Uma gestão de riscos eficaz pode ajudar a minimizar o impacto dos eventos de perda antes que eles ocorram, contribuindo para o sucesso geral dos projetos de TI (Didraga et al., 2019). No contexto dos projetos de TI, a gestão do risco é considerada um processo essencial para o sucesso da entrega do projeto (Pimchangthong & Boonjing, 2017). Foram propostos vários modelos para investigar a relação entre a gestão do risco e o sucesso do projeto, incluindo normalmente componentes como a identificação, a análise, o planeamento da resposta e a monitorização do risco (Didraga et al., 2019).

O processo de gestão de risco segundo a norma ISO 31000 é estruturado em várias etapas interligadas, que visam garantir uma abordagem sistemática e integrada à identificação, avaliação e tratamento de riscos. Inicialmente, é fundamental que a organização estabeleça um contexto claro, o que envolve entender o ambiente interno e externo, além de definir os objetivos estratégicos e operacionais. Isso permite que a gestão de risco esteja alinhada com a missão e a visão da organização (Rampini et al., 2019).

Após a definição do contexto, a identificação dos riscos é realizada. Essa etapa envolve a busca ativa por eventos ou condições que possam impactar negativamente os objetivos da organização. A identificação pode ocorrer por meio de diversas técnicas, como

brainstorming, entrevistas, e análise de documentos, entre outras (Mabrouki et al., 2014). Uma vez que os riscos são identificados, a avaliação dos mesmos se torna crucial. Nessa fase, os riscos são analisados em termos de sua probabilidade de ocorrência e do impacto potencial que poderiam causar. Essa análise pode ser qualitativa ou quantitativa, dependendo das necessidades e recursos da organização. Com os riscos identificados e avaliados, a próxima etapa é o tratamento dos riscos. Isso envolve a seleção de estratégias apropriadas para gerenciar os riscos, que podem incluir a mitigação, transferência, aceitação ou eliminação dos riscos. A escolha da estratégia deve considerar a eficácia, a eficiência e os custos envolvidos, sempre buscando a melhor relação entre risco e recompensa. Uma vez implementadas as ações de tratamento, é essencial que a organização monitore e revise continuamente os riscos e o processo de gestão de risco. Isso garante que a abordagem permaneça eficaz e adaptável às mudanças no ambiente interno e externo. Além disso, a comunicação e a consulta com as partes interessadas são fundamentais em todo o processo, garantindo que todas as vozes relevantes sejam ouvidas e que o conhecimento sobre os riscos seja compartilhado (ISO 31000, 2018). Esse processo é representado na Figura 2 a seguir:

Figura 2: Processo de Gestão de Riscos

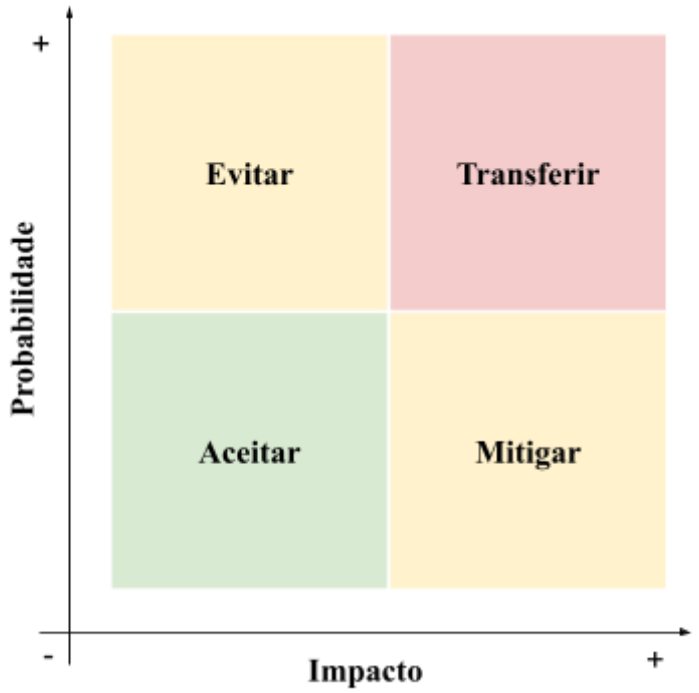


Fonte: ABNT NBR ISO/IEC 31000:2018

No contexto da gestão de riscos, existem quatro principais abordagens para tratar os riscos identificados já mencionados anteriormente, as quatro abordagens para tratar riscos são: mitigar, que envolve a implementação de ações para reduzir a probabilidade ou impacto do risco; evitar, que busca eliminar a causa do risco ou a atividade que o gera; transferir, que desloca a responsabilidade do risco para outra parte, geralmente por meio de contratos ou seguros; e aceitar, onde a organização decide não agir sobre o risco, reconhecendo sua existência e os impactos potenciais.

Para priorizar os riscos, a matriz de probabilidade e impacto é uma ferramenta eficaz que permite visualizar e categorizar os riscos de acordo com sua severidade (PMBOK, 2021). Nessa matriz (ver Figura 3), os riscos são classificados em uma grade onde a probabilidade de ocorrência é representada em um eixo e o impacto no outro, como ilustrado na figura abaixo.

Figura 3: Matriz de Probabilidade e Impacto



Fonte: Adaptado pelo autor do Guia PMBOK, 2021

Os riscos que apresentam alta probabilidade e alto impacto são considerados prioritários e devem ser tratados com urgência. Já aqueles com baixa probabilidade e baixo impacto podem ser monitorados, mas não necessitam de ação imediata. Essa abordagem

facilita a alocação de recursos de maneira eficiente e ajuda na tomada de decisões estratégicas (Duijm, 2015).

2.2. Conceitos de Segurança da Informação

Um sistema de segurança da informação é um conjunto de políticas, processos e controles implementados para proteger as informações dentro de uma organização (JOHNSON & EASTTOM, 2020). A definição enfatiza a importância da segurança em todos os níveis da infraestrutura de tecnologia da informação, integrando práticas de defesa para proteger a integridade, confidencialidade e disponibilidade (ver Figura 4) dos dados (HINTZBERGEN, 2018; LANDOLL, 2017; PELTIER, 2016).

Figura 4: Tríade da Segurança da Informação

Fonte: HINTZBERGEN, 2018

2.2.1. Confidencialidade

A confidencialidade refere-se à proteção dos dados contra o acesso não autorizado. Somente indivíduos, entidades ou sistemas que têm permissão podem acessar informações sensíveis. Para manter a confidencialidade, são utilizadas diversas técnicas e práticas, como

criptografia, controle de acesso, autenticação de usuários e políticas rigorosas de gerenciamento de senha. A confidencialidade é crucial para proteger informações pessoais, financeiras e de negócios contra espionagem, roubo de identidade e outras formas de violação de privacidade (HINTZBERGEN, 2018).

2.2.2. Integridade

A integridade garante que os dados sejam precisos e não tenham sido alterados ou corrompidos de maneira não autorizada. Isso inclui a prevenção contra modificações acidentais ou maliciosas e a manutenção da consistência dos dados ao longo do tempo. Métodos comuns para assegurar a integridade dos dados incluem o uso de somas de verificação, assinaturas digitais, controle de versão e backups regulares. A integridade é fundamental para assegurar que a informação permanece confiável e que as decisões baseadas nesses dados são fundamentadas e precisas (HINTZBERGEN, 2018).

2.2.3. Disponibilidade

A disponibilidade assegura que os sistemas, redes e dados estejam acessíveis e operacionais quando necessários. Isso significa que os usuários autorizados devem poder acessar a informação e os recursos tecnológicos de que precisam de forma consistente e confiável. Para garantir a disponibilidade, são implementadas várias práticas como redundância de sistemas, manutenção preventiva, recuperação de desastres e proteção contra ataques de negação de serviço (DDoS). A disponibilidade é vital para operações comerciais contínuas e para evitar interrupções que podem levar a perdas financeiras e reputacionais significativas (HINTZBERGEN, 2018).

2.3. Conceitos de Cibersegurança

Cibersegurança é um conjunto de práticas e tecnologias que visam proteger sistemas, redes e dados de ataques, danos ou acessos não autorizados. Ela abrange a proteção de informações confidenciais e a integridade dos sistemas, assegurando que os ativos digitais das organizações estejam resguardados contra ameaças cibernéticas (MCKINSEY & COMPANY,

2024). A gestão de riscos é essencial para a segurança da informação em uma organização, abrangendo também a área de cibersegurança, conforme ilustrado na figura 5 abaixo.

Figura 5: Relação entre Gestão de Riscos, Segurança da Informação e Cibersegurança

Fonte: Autoria própria, adaptado das bases teóricas

A NIST (*National Institute of Standards and Technology*) define a cibersegurança como a prática de proteger sistemas, redes e programas de ataques digitais. Esses ataques visam geralmente acessar, alterar ou destruir informações confidenciais, extorquir dinheiro dos usuários ou interromper processos normais de negócios.

2.3.1. Estrutura de Cibersegurança Segundo a NIST

O *National Institute of Standards and Technology* (NIST) desenvolveu uma estrutura de cibersegurança amplamente utilizada para ajudar as organizações a gerenciar e reduzir riscos associados à segurança da informação (Roy, 2020). Esta estrutura, conhecida como NIST *Cybersecurity Framework* (CSF), oferece um conjunto de diretrizes voluntárias e baseadas em práticas consagradas que promovem a proteção contra ameaças cibernéticas. A estrutura é dividida em 5 domínios (identificar, proteger, detectar, responder e recuperar) principais (ver Figura 6), 23 categorias e 108 processos. O quadro 1 apresenta as 23 categorias por seus respectivos domínios. Os 108 processos encontram-se no Anexo A no Quadro A.1.

Quadro 1: Domínio e Categoria da NIST

ID da Domínio	Domínio	ID da Categoria	Categoria
ID	Identificar	ID.AM	Gestão de Ativos
		ID.BE	Ambiente de Negócios
		ID.GV	Governança
		ID.RA	Avaliação de Riscos
		ID.RM	Estratégia de Gestão de Riscos
		ID.SC	Gestão de Riscos da Cadeia de Fornecedores
PR	Proteger	PRAC	Gestão da Identidade e Controle do Acesso
		PR.AT	Conscientização e Treinamento
		PR.DS	Segurança dos Dados
		PR.IP	Processos e Procedimentos de Proteção da Informação
		PR.MA	Manutenção
		PR.PT	Tecnologia de Proteção
DE	Detectar	DE.AE	Anomalias e Eventos
		DE.CM	Monitorização Contínua da Segurança
		DE.DP	Processos de Detecção
RS	Responder	RS.RP	Planejamento da Resposta
		RS.CO	Comunicações (Responder)
		RS.AN	Análise
		RS.MI	Mitigação
		RS.IM	Melhorias (Responder)
RC	Recuperar	RC.RP	Planeamento da Recuperação
		RC.IM	Melhorias (Recuperar)
		RC.CO	Comunicações (Recuperar)

Fonte: NIST

I. Identificar (*Identify*): A função de Identificação envolve o desenvolvimento de uma compreensão organizacional para gerenciar os riscos de cibersegurança. Isso inclui a identificação de ativos críticos, sistemas, dados e capacidades que precisam ser protegidos. Aspectos como o contexto organizacional, recursos internos e externos, e o perfil de risco da empresa são considerados para estabelecer uma base sólida.

II. Proteger (*Protect*): A função de Proteção tem como objetivo desenvolver e implementar as salvaguardas apropriadas para garantir a entrega de serviços críticos. Isso abrange controles de acesso, conscientização e treinamento de segurança, processos de proteção de dados e procedimentos de manutenção e tecnologia. O objetivo é limitar ou conter o impacto de um potencial evento de cibersegurança.

III. Detectar (*Detect*): Esta função envolve a implementação de atividades adequadas para identificar a ocorrência de eventos de cibersegurança em tempo hábil. Isso pode incluir monitoramento contínuo de sistemas e redes, detecção de anomalias e eventos, e a manutenção de processos de detecção. A capacidade de detecção eficaz permite que a organização responda rapidamente a possíveis incidentes.

IV. Responder (*Respond*): A função de Resposta foca na tomada de ações apropriadas após a detecção de um evento de cibersegurança. Isso inclui o planejamento de resposta a incidentes, comunicações, análises, mitigação e melhorias. Uma resposta coordenada e eficaz ajuda a minimizar os impactos negativos de um incidente de cibersegurança.

V. Recuperar (*Recover*): Por fim, a função de Recuperação trata da implementação de atividades para manter a resiliência e restaurar quaisquer capacidades ou serviços que foram prejudicados durante um evento de cibersegurança. Isso inclui o planejamento de recuperação, melhorias baseadas em lições aprendidas e coordenação de atividades de recuperação. O objetivo é restaurar as operações normais da organização o mais rápido possível e melhorar os planos de recuperação com base nas experiências adquiridas.

Figura 6: Estrutura de Cibersegurança

Fonte: NIST

2.4. Importância da Cibersegurança em Serviços Digitais no Setor Financeiro

No atual panorama digital, a importância da cibersegurança na salvaguarda dos serviços digitais não pode ser subestimada. Uma vez que as organizações de vários setores dependem cada vez mais das tecnologias digitais para prestar os seus serviços, a necessidade de assegurar a integridade, a confidencialidade e a disponibilidade destes sistemas tornou-se primordial (Chaudhuri & Kahyaoğlu, 2023).

O termo "*cybersecurity*" tem sido objeto de muito discurso académico e popular, com um vasto leque de definições e perspectivas. De acordo com Schiliro, 2023, a cibersegurança é uma "iniciativa de melhoria da qualidade adotada pelas organizações para monitorizar e garantir a integridade dos seus sistemas contra a entrada não autorizada [...]".

A importância da cibersegurança é essencial nos serviços digitais para garantir medidas destinadas a proteger a confidencialidade, a integridade e a disponibilidade dos ativos digitais (Schiliro, 2023). Estas medidas podem incluir controles de acesso, encriptação, procedimentos de resposta a incidentes e monitoramento de ameaças, entre outras. A cibersegurança eficaz é fundamental para salvaguardar dados sensíveis, evitar interrupções de serviço e manter a confiança dos clientes e das partes interessadas (Lamarca, 2020).

A cibersegurança tornou-se uma preocupação para o setor financeiro, uma vez que o setor financeiro se torna cada vez mais digitalizado, fica mais exposto a uma vasta gama de ciberameaças, desde o roubo de credenciais e a fraude de identidade até à manipulação de dados, ataques de *malware* e *ransomware* (Creado & Ramteke, 2020; Uddin et al., 2020). A digitalização do setor bancário e financeiro aumentou o risco de exposição a dados sensíveis

dos clientes e a informações financeiras, o que pode ter consequências devastadoras tanto para as instituições financeiras como para os seus clientes (Hasan et al., 2023). Os clientes devem ser capazes de confiar nos sistemas em mudança e ter confiança na segurança das suas transações financeiras, o que continua a ser um desafio significativo, particularmente para aqueles com atitudes mais conservadoras em relação aos avanços tecnológicos (Srinivasan & Rajarajeswari, 2021).

O Estudo de Haruna realizado em 2022, *Defending against cybersecurity threats to the payments and banking system,* mostra que o setor financeiro é consistentemente um dos setores económicos mais visados por violações de dados, com 33% dos principais ataques a visar este setor. Este fato deve-se, em grande medida, às grandes quantidades de informações pessoais e financeiras sensíveis detidas pelas instituições financeiras, bem como ao potencial de perturbação de infra-estruturas e serviços financeiros críticos.

Uma das ameaças mais significativas que o setor financeiro enfrenta é o *ransomware*, que tem sido responsável por vários ataques de alto perfil a bancos e prestadores de serviços financeiros nos últimos anos. Os cibercriminosos estão a utilizar cada vez mais técnicas sofisticadas, como a inteligência artificial e a aprendizagem de máquina, para escapar à detecção e lançar ataques mais direcionados e eficazes (Haruna et al., 2022).

Os principais ciberataques ao setor financeiro incluem:

- Roubo de credenciais e fraude de identidade: Os atacantes visam as credenciais de início de sessão e as informações pessoais dos indivíduos para obterem acesso não autorizado a contas e sistemas financeiros.
- Manipulação de dados: Os cibercriminosos podem tentar alterar ou corromper dados financeiros, levando a relatórios incorretos e à interrupção de serviços críticos.
- Ataques de *malware*: As instituições financeiras são vulneráveis a vários tipos de *malware*, como vírus, *worms* e Cavalos de Tróia, que podem ser usados para roubar dados, interromper operações ou ganhar uma posição na rede.
- *Ransomware*: Uma ameaça crescente, em que os atacantes encriptam dados sensíveis e exigem o pagamento de um resgate em troca da sua libertação, causando perturbações significativas nas empresas.

Quando os sistemas digitais de uma empresa são comprometidos, isso pode ter consequências devastadoras. As violações de dados podem expor informações sensíveis dos clientes, minando a confiança e prejudicando a reputação da empresa (Lowry et al., 1951). As

interrupções de serviço causadas por ciberataques podem afetar a capacidade da organização para servir os seus clientes, levando à perda de receitas, à perda de oportunidades de negócio e à frustração dos clientes.

Para endereçar estes riscos emergentes, os reguladores e supervisores financeiros lançaram várias iniciativas, tanto a nível nacional como internacional, para reforçar a ciber-resiliência do sistema financeiro. Estes esforços incluem a aplicação de regulamentação obrigatória em segurança da informação e cibersegurança, bem como o desenvolvimento de estratégias e técnicas de ciberdefesa ativa para proteger contra as ameaças (Creado & Ramteke, 2020).

Além disso, os órgãos reguladores e as normas do setor impõem frequentemente requisitos rigorosos em matéria de cibersegurança, e o incumprimento pode resultar em pesadas multas e repercussões jurídicas (Ramirez & Choucri, 2016).

Por outro lado, uma postura robusta em segurança da informação e cibersegurança pode melhorar a imagem de uma empresa como prestador de serviços seguro e digno de confiança (Makridis, 2021). É mais provável que os clientes confiem os seus dados e negócios a organizações que demonstrem um forte compromisso com a proteção dos seus ativos digitais. Isto, por sua vez, pode levar a uma maior fidelização dos clientes, a uma maior quota de mercado e a uma vantagem competitiva no setor (The consumer-data opportunity and the privacy imperative, 2020).

A cibersegurança não é apenas uma preocupação de TI, é um dever estratégico que deve ser adotado aos mais altos níveis de uma organização (Shen et al., 2023). Ao dar prioridade à cibersegurança e integrá-la na estratégia empresarial global, as empresas podem mitigar os riscos, proteger a sua marca e assegurar a sustentabilidade a longo prazo dos seus serviços digitais. Investir em medidas robustas de cibersegurança não é apenas um movimento defensivo, mas também um passo proativo para a construção de um ecossistema digital seguro, resiliente e centrado no cliente (Saeed et al., 2023).

2.5. Visão Geral das Normas ISO 27001 e ISO 27002

A ISO 27001 e a ISO 27002 são normas internacionais que fornecem uma estrutura abrangente para sistemas de gestão da segurança da informação. Estas normas ganharam reconhecimento e adoção generalizados em todo o mundo, servindo como uma linguagem

comum para as organizações abordarem as suas responsabilidades em matéria de segurança da informação (Culot et al., 2021).

A norma ISO 27001, formalmente conhecida como “ISO/IEC 27001 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos”, descreve os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação numa organização. Esta norma realça a importância de uma abordagem sistemática para gerir ativos de informação sensíveis, assegurar a continuidade do negócio e minimizar potenciais perdas (ISO 27001, 2022).

Por outro lado, a norma ISO 27002, intitulada "ISO/IEC 27002 - Tecnologia da informação - Técnicas de segurança - Código de práticas para controles de segurança da informação", fornece um conjunto de melhores práticas e diretrizes para a implementação de controles de segurança da informação. Esses controles abrangem uma ampla gama de áreas, incluindo controle de acesso, criptografia, segurança física, segurança de operações e gerenciamento de incidentes de segurança da informação, entre outras (ISO 270002, 2022).

2.5.1. ISO/IEC 27001

A ISO/IEC 27001 é uma norma internacionalmente reconhecida que especifica os requisitos para a criação, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Segurança da Informação (SGSI) dentro do contexto da organização. Seu principal objetivo é ajudar as organizações a protegerem suas informações de forma sistemática e eficaz, abordando os riscos de segurança da informação através de seus requisitos e controles (ISO 27001, 2022). A figura 7 ilustra de forma visual os requisitos da norma.

Figura 7: Requisitos da ISO 27001:2022

Fonte: Adaptado pelo autor da ABNT NBR ISO/IEC 27001:2022

A ISO/IEC 27001 é estruturada em várias seções que cobrem todos os aspectos necessários para a criação, implementação, manutenção e melhoria contínua de um SGSI. Estas seções estão abaixo no Quadro 2:

Quadro 2: Descrição dos Requisitos da ISO 27001:2022

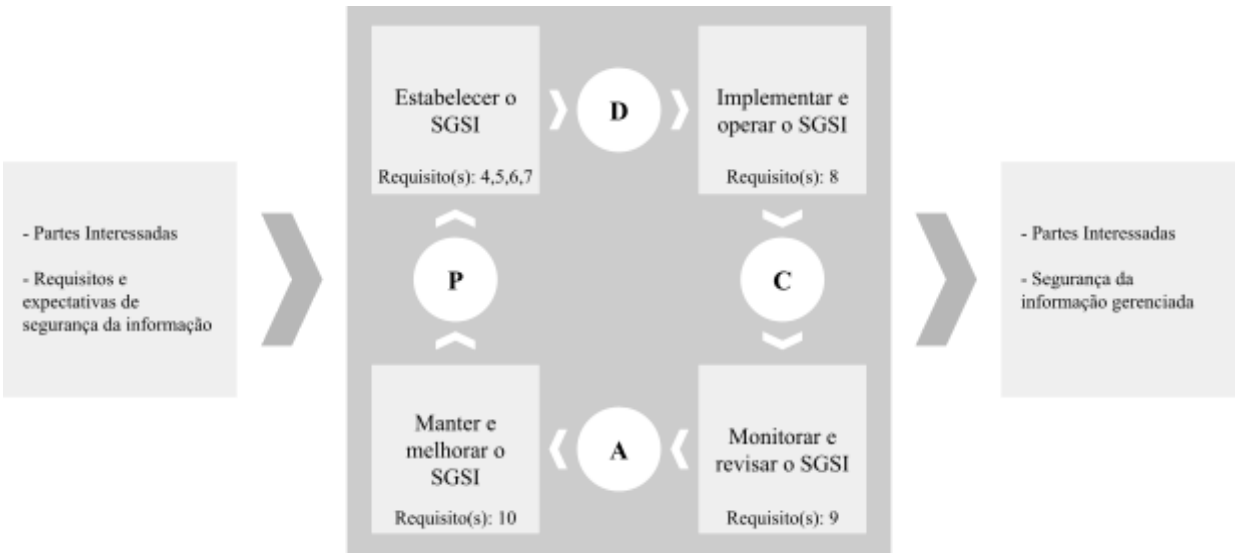
Requisitos	**Descrição**
4. Contexto da Organização	Compreensão do contexto interno e externo da organização, identificação das partes interessadas e definição do escopo do SGSI.

5. Liderança	Comprometimento da alta direção, estabelecimento de políticas de segurança da informação e definição clara de papéis e responsabilidades.
6. Planejamento	Identificação e avaliação de riscos e oportunidades, definição de objetivos de segurança e planejamento de ações para tratar os riscos.
7. Suporte	Disponibilização de recursos, treinamento e conscientização, comunicação e controle de documentação.
8. Operação	Implementação e controle das operações planejadas, gestão de riscos e mudanças, e condução das operações diárias.
9. Avaliação de Desempenho	Monitoramento e medição da eficácia do SGSI, auditorias internas e revisões pela direção.
10. Melhoria	Implementação de ações corretivas e busca pela melhoria contínua do SGSI.

Fonte: Adaptado pelo autor da ABNT NBR ISO/IEC 27001:2022

A ISO/IEC 27001 é baseada no ciclo PDCA (ver Figura 8), também chamado de roda de Deming ou ciclo de Shewhart, um modelo iterativo desenvolvido para alcançar a melhoria contínua (Aldya et al., 2019). Esse modelo foi criado em torno de 1939 pelo engenheiro, físico e estatístico Walter Andrew Shewhart, e mais tarde popularizado pelo estatístico W. Edwards Deming.

Figura 8: Ciclo PDCA de SGSI



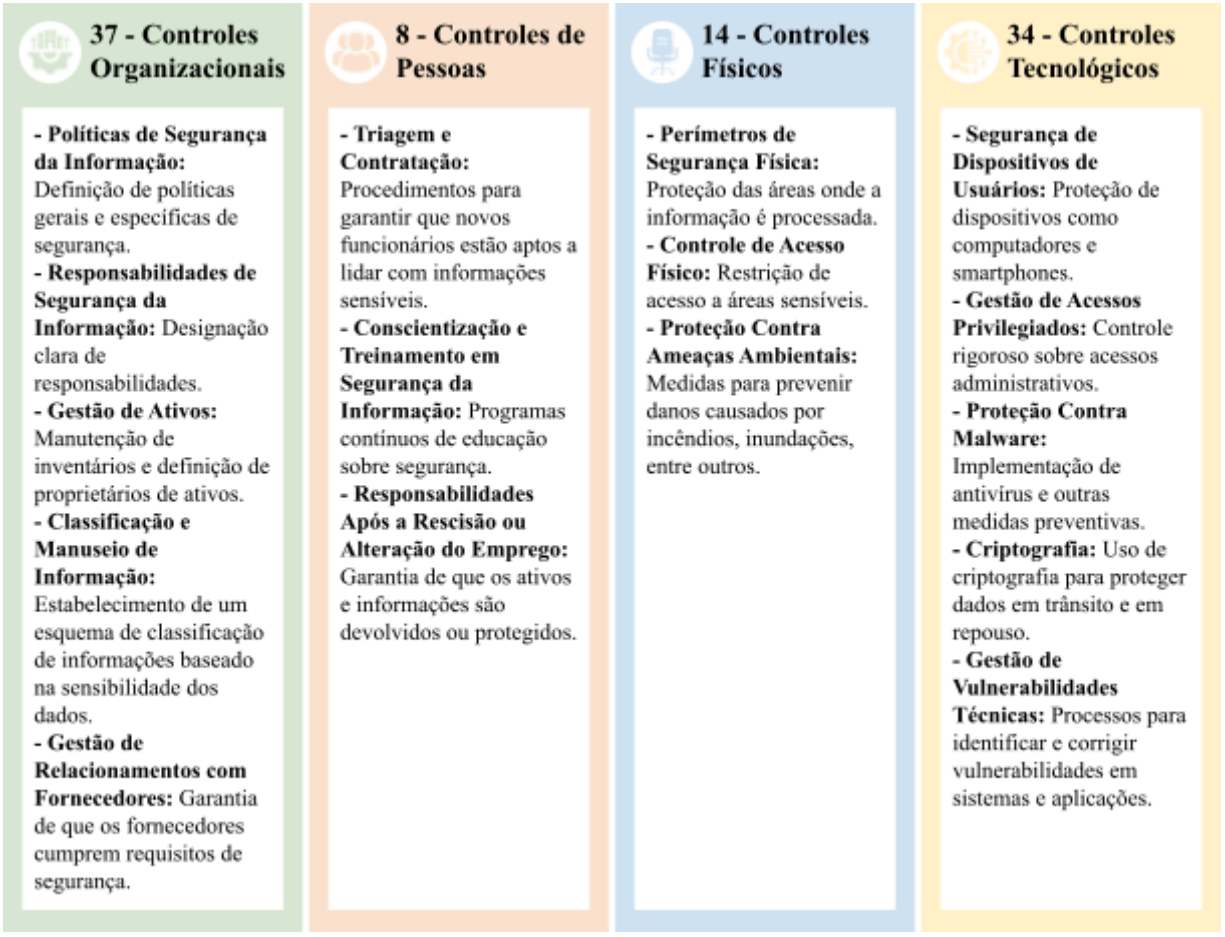
Fonte: Adaptado pelo autor da ABNT NBR ISO/IEC 27001:2022

A implementação da ISO/IEC 27001 no contexto da cibersegurança é um processo estratégico e sistemático que visa proteger os ativos de informação contra ameaças cibernéticas, é um processo detalhado e contínuo que ajuda as organizações a proteger seus ativos de informação de maneira eficaz. Ao seguir os princípios e controles estabelecidos pela norma, as empresas podem não apenas mitigar riscos, mas também melhorar sua resiliência e confiança perante as suas partes interessadas.

2.5.2. ISO/IEC 27002

A ISO/IEC 27002 é uma norma internacional que fornece diretrizes para a implementação de controles de segurança da informação. Seu objetivo é complementar a ISO/IEC 27001, detalhando os controles (ver Figura 9) que podem ser aplicados para mitigar riscos identificados (DISTERER, 2013). A norma é dividida em várias seções que abordam diferentes tipos de controles: organizacionais, de pessoas, físicos e tecnológicos.

Figura 9: Tipos de Controles da ISO 27002:2022



Fonte: Adaptado pelo autor da ABNT NBR ISO/IEC 27002:2022

A ISO/IEC 27002 segue as diretrizes estabelecidas pela ISO/IEC 27001, sendo uma extensão prática desta norma. Enquanto a ISO/IEC 27001 define os requisitos para estabelecer, implementar, manter e melhorar continuamente um SGSI, a ISO/IEC 27002 fornece um guia detalhado sobre como implementar os controles de segurança especificados na ISO/IEC 27001. A implementação dos controles descritos na ISO/IEC 27002 deve ser realizada de forma a atender às necessidades específicas da organização. Para isso, é essencial seguir os seguintes passos (ver Quadro 3):

Quadro 3: Descrição dos Passos de Implementação da ISO 27002:2022

Passos	**Descrição**
Avaliação de Riscos	Identificar e avaliar os riscos específicos para a organização.

Seleção de Controles	Escolher os controles apropriados com base na avaliação de riscos.
Implementação	Colocar em prática os controles selecionados, garantindo que todos os funcionários estejam cientes de suas responsabilidades.
Monitoramento e Revisão	Realizar monitoramento contínuo e revisar regularmente os controles para garantir sua eficácia

Fonte: Adaptado pelo autor da ABNT NBR ISO/IEC 27002:2022

2.5.3. Diferenciais Entre as Duas ISOs

A ISO/IEC 27001 e a ISO/IEC 27002 são normas complementares no campo da segurança da informação, mas possuem objetivos e estruturas distintas.

A ISO/IEC 27001 é uma norma de requisitos, voltada para a certificação e auditoria de um Sistema de Gestão de Segurança da Informação (SGSI). Esta norma estabelece uma estrutura para identificar, avaliar e tratar riscos de segurança da informação, garantindo a proteção de dados sensíveis. A ISO/IEC 27001 é baseada no ciclo PDCA (Plan-Do-Check-Act), que promove a melhoria contínua do SGSI. Seus requisitos cobrem desde a definição do escopo do SGSI até a avaliação de desempenho e ações corretivas, proporcionando uma abordagem sistemática para gerenciar a segurança da informação (Aldya et al., 2019).

Por outro lado, a ISO/IEC 27002 serve como um guia prático para a implementação dos controles de segurança especificados na ISO/IEC 27001. Enquanto a ISO/IEC 27001 define o "o quê" deve ser feito, a ISO/IEC 27002 detalha o "como" fazê-lo. Ela oferece diretrizes detalhadas e exemplos de boas práticas para a implementação dos controles de segurança, ajudando as organizações a adaptar os controles às suas necessidades específicas (DISTERER, 2013).

A diferença fundamental entre as duas normas reside em seu propósito e aplicabilidade. A ISO/IEC 27001 é essencial para a certificação, pois fornece os requisitos que uma organização deve cumprir para ser certificada como estando em conformidade com a norma. Ela foca em estabelecer, implementar, manter e melhorar um SGSI de forma contínua e sistemática, abrangendo políticas, processos e responsabilidades organizacionais (HINTZBERGEN, 2018). O Quadro 4 mostra de forma visual essas diferenças.

Quadro 4: Diferenças entre a ISO 27001 e a ISO 27002

Critério	**ISO 27001**	**ISO 27002**
Direcional	Estratégico	Prático
Objetivo	Define exigências para a implementação e manutenção de um SGSI.	Oferece diretrizes práticas para a aplicação de controles de segurança.
Foco	Baseada no ciclo PDCA (Plan-Do-Check-Act).	Descrição detalhada de controles específicos de segurança.
Estrutura	Voltada para gestores com o objetivo de criar e aprimorar o SGSI.	Baseada em boas práticas divididas por domínios de segurança.
Aplicação	Focada em gestores para criação e melhoria do SGSI.	Destinada a profissionais técnicos para implementação de controles.
Escopo	Envolve as políticas de segurança da informação e a gestão de riscos.	Enfatiza a implementação dos controles recomendados.
Certificação	Certificável; permite que as organizações sejam submetidas a auditorias.	Não certificável; serve como orientação prática.
Atualização	ISO 27001:2022.	ISO 27002:2022.

Fonte: Adaptado pelo autor das ISOs e bases teóricas

2.6. Benefícios da Implementação das Normas

No cenário digital em rápida evolução, as empresas que oferecem serviços digitais estão a reconhecer cada vez mais a importância primordial de práticas robustas de segurança da informação para salvaguardar os seus ativos, manter a confiança dos clientes e garantir a conformidade regulamentar. As duas normas internacionalmente reconhecidas, a ISO 27001 e a ISO 27002, surgiram como estruturas essenciais para estabelecer e manter Sistemas de Gestão da Segurança da Informação eficazes nas organizações (Boehmer, 2008; Okpamen, 2013; Culot et al., 2021).

A implementação destas normas oferece uma infinidade de benefícios para as empresas digitais. Em primeiro lugar, a adoção das normas ISO 27001 e ISO 27002

proporciona uma abordagem abrangente e estruturada para identificar, avaliar e mitigar os riscos de segurança da informação. Este processo sistemático de gestão do risco permite que as empresas digitais abordem proativamente as potenciais ameaças, reduzindo a probabilidade de violações de dados dispendiosas, ciberataques e outros incidentes de segurança (Jakábová et al., 2013).

Adicionalmente, a implementação das normas ISO 27001 e ISO 27002 pode fornecer às empresas digitais um enquadramento para a melhoria contínua das suas práticas de segurança da informação. Estas normas exigem que as organizações revejam e atualizem regularmente os seus controles de segurança, garantindo que estes permanecem eficazes perante as ameaças e das alterações regulamentares. Este compromisso de melhoria contínua pode conduzir a uma postura de segurança mais resiliente e adaptável, mais bem equipada para resistir e responder aos desafios emergentes em matéria de cibersegurança (Kitsios et al., 2022).

Além disso, a adoção destas normas pode ter um impacto positivo na eficiência operacional das empresas digitais. Ao estabelecer funções, responsabilidades e processos claros para a gestão da segurança da informação, a ISO 27001 e a ISO 27002 podem ajudar a simplificar as atividades relacionadas com a segurança, reduzir a duplicação de esforços e otimizar a atribuição de recursos. Isso, por sua vez, pode resultar em maior produtividade, economia de custos e uma utilização mais eficaz do pessoal de segurança e dos investimentos em tecnologia da empresa (Okpamen, 2013).

Estas normas reconhecidas globalmente funcionam como um fator de diferenciação, tornando as empresas digitais que obtiveram a certificação mais atrativa para potenciais clientes e parceiros comerciais. O alinhamento com as melhores práticas do setor inspira uma maior confiança nos clientes, parceiros e partes interessadas, conduzindo a uma melhor reputação e à fidelização dos clientes. Isto pode ajudar as empresas digitais a destacarem-se dos seus concorrentes e a assegurar novas oportunidades de negócio, reforçando, em última análise, a sua posição no mercado e impulsionando o crescimento (Panda, 2019). O quadro 5 ilustra os principais benefícios encontrados.

Quadro 5: Benefícios da Implementação da ISO 27001:2022

Benefícios	**Descrição**
Gestão abrangente de riscos	A abordagem estruturada para identificar, avaliar e mitigar os riscos de

	segurança da informação permite que as empresas digitais abordam proativamente as potenciais ameaças (Boehmer, 2008; Okpamen, 2013; Culot et al., 2021; Jakábová et al., 2013).
Melhoria da reputação e da confiança	O alinhamento com as melhores práticas do setor inspira maior confiança nos clientes, parceiros e partes interessadas, levando a uma melhor reputação e à fidelização dos clientes (Panda, 2019).
Vantagem competitiva	O reconhecimento global destas normas pode servir como um fator de diferenciação, tornando as empresas digitais mais atrativas para potenciais clientes e parceiros comerciais (Panda, 2019).
Conformidade simplificada	A adesão aos princípios das normas ISO 27001 e ISO 27002 pode simplificar o processo de conformidade regulamentar, reduzindo a carga administrativa e as potenciais penalizações legais ou financeiras (Okpamen, 2013).
Cultura consciente de segurança	O quadro estruturado incentiva os funcionários de todos os níveis a participarem ativamente na proteção dos ativos da organização, melhorando a postura geral de segurança (Kitsios et al., 2022).

Fonte: Adaptado pelo autor das bases teóricas

Para implementar as normas ISO/IEC 27001 e ISO/IEC 27002 de forma eficaz, é essencial utilizar os 5W+1H (*What, Why, When, Who, Where, How*).

2.6.1. 5W+1H

Essa abordagem permite definir detalhadamente os aspectos críticos da implementação, incluindo o que precisa ser feito (*What*), por que é necessário (*Why*), quem será responsável (*Who*), quando as ações serão realizadas (*When*), onde as atividades ocorrerão (*Where*), e como as ações serão executadas (*How*). Essa estrutura sistemática (ver Quadro 6) ajuda a garantir que todos os aspectos da implementação sejam planejados e geridos de maneira eficiente, facilitando a conformidade total com as normas (How to Use the 5W1H Rule?, 2023).

Quadro 6: 5W+1H

Objetivo	**Detalhamento**

What	Identifica o que precisa ser feito, descrevendo a ação ou tarefa específica a ser realizada.	O que precisa ser feito? Qual é a ação específica a ser tomada? Quais são as tarefas envolvidas?
Why	Explica a razão pela qual a ação é necessária, detalhando os objetivos e a importância da tarefa.	Por que esta ação é necessária? Por que você está mirando em um objetivo específico?
Who	Define quem será responsável pela execução da ação, identificando os indivíduos ou equipes envolvidos.	Quem será responsável pela execução da ação? Quem está envolvido no projeto? Quem são as partes interessadas?
When	Determina o prazo para a execução da ação, estabelecendo cronogramas e datas de início e término.	Quanto tempo dura? Quando é o prazo para a conclusão? Quais são as datas-chave e marcos?
Where	Especifica o local onde a ação será realizada, seja um local físico ou um sistema específico.	Onde a ação será realizada? Qual é o local específico (físico ou virtual)?
How	Descreve como a ação será executada, detalhando os métodos, processos e recursos necessários.	Como a ação será executada? Como os recursos serão utilizados e gerenciados?

Fonte: Adaptado pelo autor do *How to Use the 5W1H Rule?*, 2023

Ao colocar estas questões, os indivíduos e as equipes podem obter uma compreensão mais abrangente do problema em causa, identificar as principais partes interessadas, determinar os fatos e os detalhes relevantes e descobrir as causas e motivações subjacentes. Esta abordagem holística ajuda a garantir que todos os aspectos importantes do problema são considerados, conduzindo a soluções mais eficazes e bem informadas (5W1H Glossary: Definition, Method and Practical Use, 2023).

O 5W+1H pode ser aplicado em uma variedade de situações, desde o desenvolvimento de estratégias empresariais à investigação científica e à tomada de decisões pessoais (Su, 2014). É uma ferramenta versátil que pode ser adaptada às necessidades e requisitos específicos de qualquer problema ou cenário.

Uma das principais vantagens do 5W+1H é a sua ênfase na análise da causa raiz. O método está também estreitamente ligado ao conceito de uma "abordagem baseada na eficácia" para a resolução de problemas, tal como descrito por Kettner, Moroney e Martin no

seu trabalho "*Designing and Managing Programs: An Effectiveness-Based Approach*" (Knepper, 2009). Esta abordagem enfatiza a importância de se concentrar nos elementos mais essenciais de um problema, em vez de simplesmente abordar os serviços ou soluções que já estão em vigor.

3. METODOLOGIA

A metodologia deste trabalho é conduzida em formato de estudo de caso, focado na segurança da informação de uma empresa do setor financeiro que oferece serviços digitais. A metodologia inclui a coleta de dados internos e externos, envolvendo a análise de documentos, políticas e procedimentos de segurança da informação da organização. Além disso, foi realizada uma revisão da literatura para entender como esses conceitos se refletem nas bases teóricas. Serão também conduzidas entrevistas com funcionários em diferentes níveis para compreender a percepção e a implementação das práticas de segurança na empresa. Essa abordagem permitirá uma visão abrangente do nível de conformidade e das áreas que necessitam de melhorias.

3.1. Tipo de Pesquisa

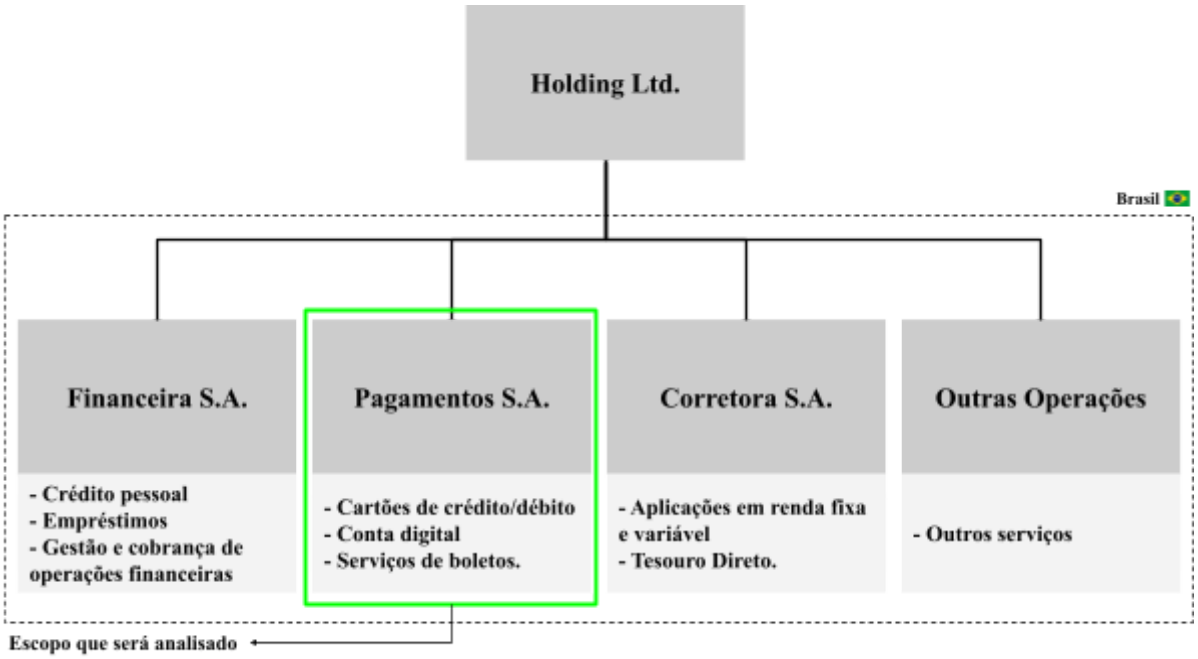
O tipo de pesquisa envolve a revisão da literatura e o estudo de caso, proporcionando uma análise detalhada e contextualizada da segurança da informação na organização.

3.2. Descrição da Empresa Analisada

A empresa em questão possui capital aberto e, devido a restrições de confidencialidade, não é possível fornecer muitos detalhes específicos sobre sua identidade. No entanto, podemos afirmar que ela opera no setor financeiro, oferecendo diversos serviços digitais aos seus clientes. A organização oferece uma ampla gama de serviços digitais que abrangem várias áreas tecnológicas, atendendo a uma base diversificada de clientes.

A análise focará em avaliar a segurança da informação dentro dessa empresa, utilizando dados internos e externos para fornecer um diagnóstico abrangente. Devido aos requisitos do diagnóstico estabelecido pela norma ISO, é essencial delimitar o escopo da análise. Dessa forma, o escopo será limitado às operações de Pagamentos S.A. (ver Figura 10), visto que esta estrutura é a mais consolidada dentro da empresa. Tal abordagem permitirá maior precisão e agilidade na realização do diagnóstico, facilitando o processo e garantindo resultados mais claros e objetivos.

Figura 10: Escopo de Pesquisa



Fonte: Autoria própria

3.3. Coleta de Dados

A coleta de dados incluirá informações internas e externas da organização. As informações internas serão obtidas através de entrevistas com quatro funcionários-chave: um Diretor de Engenharia, um Gerente de Riscos de Tecnologia da Informação, um Gerente de Segurança da Informação e um Gerente de Engenharia (ver Quadro 7). Cada entrevista terá uma duração média de 30 minutos. Além disso, serão analisados relatórios, *dashboards* e planilhas relacionados aos controles existentes. As informações externas serão coletadas a partir de relatórios públicos divulgados pela empresa, que possui capital aberto.

Quadro 7: Identificação dos Entrevistados

Identificação	**Cargo**
E1	Diretor de Engenharia
E2	Gerente de Riscos de Tecnologia da Informação
E3	Gerente de Segurança da Informação

E4	Gerente de Engenharia

Fonte: Autoria própria

O questionário visa obter percepções detalhadas sobre a eficácia dos controles de segurança da informação implementados e identificar possíveis áreas de melhoria. O questionário utilizado está disponível no Apêndice A, ao final do trabalho. Esse método de pesquisa permitirá uma compreensão aprofundada e contextualizada das práticas de segurança da informação da empresa, proporcionando uma base sólida para a análise e as recomendações subsequentes.

As entrevistas foram conduzidas seguindo uma estrutura aberta, permitindo que os entrevistados tivessem liberdade para expor suas respostas de forma espontânea. Esse formato incentivou um diálogo mais fluido e a expressão de opiniões e experiências pessoais, contribuindo para uma visão mais rica e variada do cenário atual da segurança da informação na empresa.

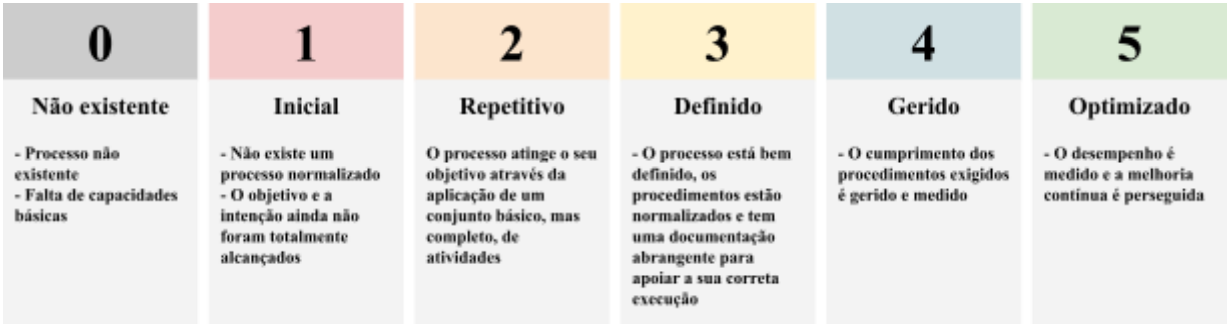
As análises das respostas foram realizadas de maneira qualitativa, sem a utilização de *softwares* específicos para análise. O foco esteve nas respostas obtidas e nas anotações feitas durante as entrevistas, o que possibilitou uma interpretação mais próxima do contexto e das nuances das opiniões dos entrevistados. Essa abordagem qualitativa assegura que as recomendações subsequentes sejam fundamentadas em uma compreensão mais profunda das percepções e experiências dos participantes.

Para diagnosticar a percepção da companhia, foi utilizado a estrutura de cibersegurança da NIST, que conta com um total de 108 processos. Esses processos serviram não só para analisar como a empresa se vê em relação a segurança da informação, mas também ajudaram na percepção em relação às normas, visto que há similaridade entre alguns processos do NIST e os requisitos das normas ISO 27001 e ISO 27002. Para auxiliar na recomendação do plano de ação, foi feita uma avaliação dos 108 processos, juntamente com o time de Segurança da Informação, para 46 responsáveis em 15 unidades de negócios. O objetivo foi identificar o nível das capacidades e maturidade de segurança, conforme definições estabelecidas pela Estrutura de Cibersegurança da NIST, que já é utilizado atualmente pela companhia, categorizando-os dentro dos cinco domínios (identificar, proteger, detectar, responder e recuperar). O Quadro A.1 no Anexo A apresenta todos os processos categorizados por sua respectiva categoria e domínio.

Trabalharemos com as médias totais em cada domínio e cada categoria, segregadas em duas visões: uma visão do time de Segurança da Informação e outra dos demais times, a fim de comparar as notas.

Além disso, para a avaliação, o time de Segurança da Informação definiu uma escala de maturidade dos processos (ver Figura 11) para determinar a pontuação de cada processo, onde a escala 3 foi atribuída como o mínimo exigido para que os processos estejam bem definidos.

Figura 11: Escala de maturidade dos processos



Fonte: Autoria própria

Dessa forma, conseguimos entender o momento em que a empresa se encontra em relação à estrutura de NIST para propor um plano de ação adequado.

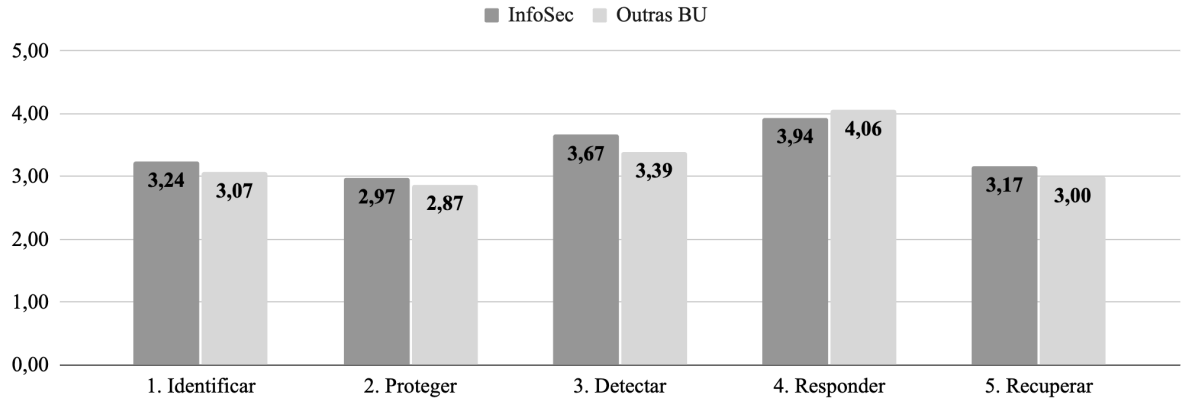
4. DIAGNÓSTICO E ANÁLISE DA EMPRESA

Neste tópico de diagnóstico da empresa, será apresentada uma análise detalhada da situação atual da segurança da informação na organização, com foco nos pontos fortes e fracos identificados. A partir dessa avaliação, será possível identificar as áreas de melhoria e sugerir ações corretivas para garantir maior conformidade com as normas ISO/IEC 27001 e ISO/IEC 27002, além de reforçar a postura de segurança digital da empresa.

4.1. Diagnóstico Atual da Empresa

Em primeiro lugar, iremos analisar a percepção da empresa em relação à estrutura de cibersegurança da NIST. Com base nas respostas relativas aos 108 processos, pudemos categorizá-los entre os domínios da NIST (Identificar, Proteger, Detectar, Responder e Recuperar) e segregá-los em duas visões: uma do time de Segurança da Informação e outra dos demais times, conforme ilustrado na figura 12.

Figura 12: Gráfico de Avaliação dos Domínios da NIST



Fonte: Autoria própria

Analisando o gráfico sobre a avaliação dos domínios NIST, podemos observar várias informações importantes. No domínio "Identificar", o time de Segurança da Informação (InfoSec) obteve uma nota média de 3,24, enquanto as outras Unidades de Negócio (BUs) receberam uma nota média de 3,07. As notas são muito próximas, indicando que tanto o InfoSec quanto as outras BUs têm uma visão similar sobre a capacidade de identificar riscos.

No domínio "Proteger", o InfoSec apresentou uma nota média de 2,97, em comparação com 2,87 das outras BUs. Isso sugere que o time de Segurança da Informação avalia suas capacidades de proteção um pouco melhor do que as outras BUs, mas ambas as notas estão abaixo de 3, indicando uma área com potencial para melhorias.

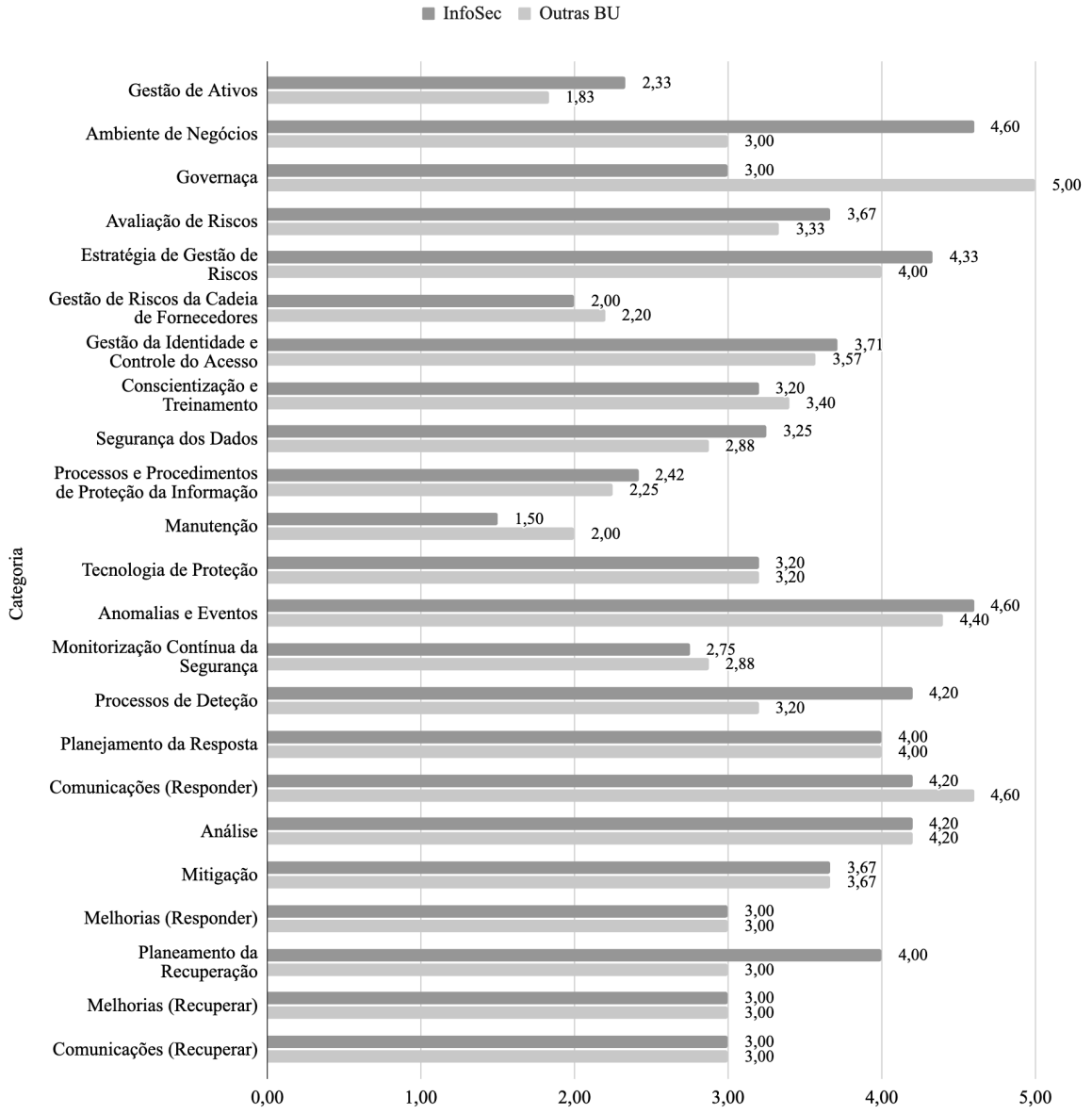
No domínio "Detectar", o InfoSec teve uma nota média de 3,67, enquanto as outras BUs ficaram com 3,39. Ambas as avaliações são acima de 3, sugerindo que há uma percepção de que a capacidade de detecção é adequada, mas ainda há espaço para aprimoramento.

No domínio "Responder", o InfoSec recebeu uma nota média de 3,94, enquanto as outras BUs tiveram uma nota de 4,06. As outras BUs têm uma visão mais positiva sobre sua capacidade de resposta em comparação com InfoSec, mas ambas estão próximas de 4, indicando uma percepção relativamente boa.

Por fim, no domínio "Recuperar", o InfoSec obteve uma nota média de 3,17, enquanto as outras BUs tiveram uma nota média de 3. As avaliações estão próximas e ligeiramente acima de 3, mostrando que a recuperação é vista como um ponto relativamente forte, mas ainda há oportunidades para melhorias.

Comparando de forma geral, em alguns dos domínios, as avaliações de InfoSec são ligeiramente superiores às das outras BUs, sugerindo que o time de Segurança da Informação pode ter mais confiança nas suas capacidades ou talvez tenha uma visão mais otimista. O domínio "Proteger" apresenta notas mais baixas em comparação aos outros, indicando que podem ser áreas prioritárias para melhorias e desenvolvimento. Por outro lado, a capacidade de "Responder" é vista como um ponto forte, especialmente por outras BUs.

Figura 13: Gráfico de Avaliação das Categorias da NIST



Fonte: Autoria própria

A análise do gráfico da figura 13 revela a percepção da empresa em relação a várias categorias da estrutura de cibersegurança da NIST, comparando a visão do time de Segurança da Informação (InfoSec) com a dos demais times (Outras BU).

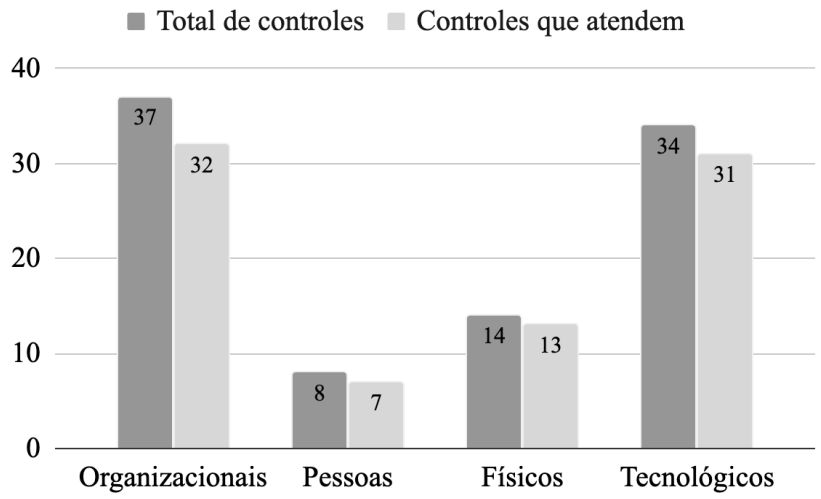
A categoria de Manutenção apresentou as menores avaliações, com o time de InfoSec atribuindo uma pontuação de 1,50, enquanto as outras unidades de negócios deram uma nota ligeiramente superior de 2,00. Na Gestão de Ativos, a pontuação foi de 2,33 pelo time de InfoSec e 1,83 pelas outras BU, destacando uma percepção negativa em ambas as visões. Para

a Gestão de Riscos da Cadeia de Fornecedores também teve baixa avaliação, com 2,00 pelo time de InfoSec e 2,20 pelas outras BU, sugerindo que a documentação e os procedimentos precisam ser aprimorados. Os Processos e Procedimentos de Proteção receberam pontuações de 2,42 e 2,25 pelo time de InfoSec e outras BU, respectivamente, apontando para a necessidade de melhorias na documentação e implementação de processos.

Essas categorias, com as menores pontuações de avaliação pelo time de Segurança da Informação e também relativamente baixas nas avaliações das outras unidades de negócios, sugerem que essas áreas podem necessitar de atenção especial em termos de documentação e procedimentos para melhorar a percepção e a eficácia da segurança dentro da empresa. Os pontos foram evidenciados também durante a análise dos controles em relação às normas, salientando principalmente a necessidade de melhorar a comunicação e a documentação.

Em segundo lugar, a análise dos resultados obtidos a partir da avaliação dos controles de segurança da informação da norma ISO/IEC 27001 revelou uma forte aderência com os controles da norma (ver Figura 14).

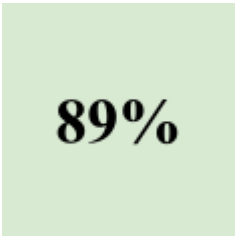
Figura 14: Gráfico de Aderência dos Tipos de Controles da ISO 27001:2022



Fonte: Autoria própria

Dos 93 controles especificados pela norma, a empresa demonstrou aderência a 89% (ver Figura 15), o que representa uma conformidade substancial com as diretrizes de segurança.

Figura 15: Percentual de Aderência dos Controles da ISO 27001:2022



Fonte: Autoria própria

Essa alta taxa de aderência indica que a empresa tem implementado de forma eficaz a maioria dos controles recomendados, refletindo um compromisso robusto com a proteção das informações. No entanto, é importante identificar e abordar os 11% dos controles que ainda não foram plenamente adotados para garantir a conformidade total e fortalecer ainda mais a postura de segurança da organização. Abaixo no Quadro 8 temos a análise completa dos 93 controles, com as informações sobre o controle, o diagnóstico e as evidências.

Quadro 8: Detalhamento do Diagnóstico de Cada um dos Controles da ISO 27001:2022

5	**Controles Organizacionais**		**Requisito**	**Evidência**
5.1	Políticas para Segurança da Informação	**Controle** Política de Segurança da Informação e políticas de tópicos específicos devem ser definidas, aprovadas pela gestão, publicadas, comunicadas, reconhecidas por partes interessadas relevantes e revisadas em intervalos planejados, no momento em que mudanças significativas ocorrerem.	**Atende**	Arquivo em PDF disponibilizado internamente e externamente para a companhia.
5.2	Papéis e Responsabilidades de Segurança da Informação	**Controle** Papéis e responsabilidades de Segurança da Informação devem ser definidos e alocados de acordo com as necessidades da organização.	**Atende**	Definição clara de papéis e responsabilidades documentada em PDF.
5.3	Segregação de Funções	**Controle** Funções e áreas de responsabilidade conflitantes devem ser segregadas.	**Atende**	Procedimentos documentados e armazenados no sistema interno.
5.4	Responsabilidades de Gestão	**Controle** A Administração deve exigir que todos os colaboradores apliquem Segurança da Informação de acordo com a Política de Segurança da Informação estabelecida, políticas de tópicos específicos e procedimentos da organização.	**Atende**	Responsabilidades documentadas em políticas internas e comunicadas aos gestores.

5.5	Contato com Autoridades	**Controle** A organização deve estabelecer e manter contato com autoridades relevantes.	**Atende**	Contatos documentados e registrados em banco de dados acessível.
5.6	Contato com Grupos de Interesses Especiais	**Controle** A organização deve estabelecer e manter contato com grupos de interesses especiais, fóruns de especialistas em segurança e associações profissionais.	**Não Atende**	Ausente
5.7	Inteligência contra Ameaças	**Controle** Informações relacionadas às ameaças de Segurança da Informação devem ser coletadas e analisadas, a fim de produzir inteligência contra ameaças.	**Não Atende**	Ausente
5.8	Segurança da Informação no Gerenciamento de Projetos	**Controle** Segurança da Informação deve integrar-se ao gerenciamento de projetos.	**Atende**	Políticas documentadas e disponíveis em sistema interno.
5.9	Inventário de Informações e outros Ativos Associados	**Controle** Um inventário de informações e outros ativos associados, incluindo proprietários, deve ser desenvolvido e mantido.	**Não Atende**	Ausente
5.10	Uso Aceitável da Informação e outros Ativos Associados	**Controle** Regras para o uso aceitável e procedimentos para o manuseio de informações e outros ativos associados devem ser identificadas, documentadas e implementadas.	**Atende**	Políticas de uso aceitável documentadas e comunicadas aos

				funcionários.
5.11	Devolução de Ativos	**Controle** Colaboradores e outras partes interessadas devem devolver todos os ativos organizacionais que estejam em sua posse em caso de mudança ou término de seus empregos, contratos ou acordos.	**Atende**	Procedimentos documentados e seguidos para devolução de ativos.
5.12	Classificação das Informações	**Controle** Informações devem admitir classificação de acordo com as necessidades da organização em Segurança da Informação, baseadas nos requisitos de confidencialidade, integridade e disponibilidade das partes interessadas relevantes.	**Atende**	Documentação de classificação de informações em PDF.
5.13	Rotulagem das Informações	**Controle** Um conjunto adequado de procedimentos para rotulagem das informações deve ser desenvolvido e implementado, de acordo com o esquema de classificação das informações adotado pela organização.	**Atende**	Políticas de rotulagem documentadas e aplicadas.
5.14	Transferência das Informações	**Controle** Regras, procedimentos e acordos de transferência das informações devem ocorrer em todos os tipos de instalações de transferência na organização, entre ela e partes interessadas.	**Atende**	Procedimentos documentados e monitorados para transferência de informações.
5.15	Controle de Acesso	**Controle** Regras para o controle físico e lógico de acesso às informações e outros ativos associados devem ser estabelecidos e implementados,	**Atende**	Políticas de controle de acesso documentadas e implementadas.

		conforme os requisitos de negócio e Segurança da Informação.		
5.16	Gerenciamento de Identidade	**Controle** O ciclo de vida completo das identidades deve ser gerenciado.	**Atende**	Sistema de gestão de identidades implementado e monitorado.
5.17	Informações de Autenticação	**Controle** Alocação das informações de autenticação deve admitir controle por um processo de gerenciamento, incluindo aconselhamento aos colaboradores a respeito do manuseio adequado de informações de autenticação.	**Atende**	Políticas de autenticação documentadas e aplicadas.
5.18	Direitos de Acesso	**Controle** Direitos de acesso a informações e outros ativos associados devem ser provisionados, revisados, modificados e removidos, de acordo com políticas de tópicos específicos da organização e regras para controle de acesso.	**Atende**	Revisão periódica dos direitos de acesso de usuários realizada e registrada.
5.19	Segurança da Informação em Relacionamentos com Fornecedores	**Controle** Processos e procedimentos devem ser definidos e implementados, a fim de gerenciar os riscos de Segurança da Informação associados com o uso de produtos ou serviços de fornecedores.	**Atende**	Política de segurança de fornecedor não formalizada.
5.20	Abordagem da Segurança da Informação nos Contratos com Fornecedores	**Controle** Requisitos relevantes de Segurança da Informação devem ser estabelecidos e acordados com cada fornecedor, conforme os seus	**Atende**	Requisitos de segurança em contratos com fornecedores

		tipos de relacionamento.		estabelecidos e documentados.
5.21	Gerenciamento de Segurança da Informação na Cadeia de Suprimentos de Tecnologia da Informação e Comunicação (TIC)	**Controle** Processos e procedimentos devem ser definidos e implementados, a fim de gerenciar os riscos de Segurança da Informação associados com os produtos e serviços de TIC da cadeia de suprimentos.	**Atende Parcialmente**	Procedimentos de gestão de segurança da cadeia de suprimentos de TIC não documentados.
5.22	Monitoramento, Revisão e Gerenciamento de Mudanças de Serviços de Fornecedores	**Controle** A organização deve regularmente monitorar, revisar, avaliar e gerenciar mudanças nas práticas de Segurança da Informação dos fornecedores e na entrega de serviços.	**Atende Parcialmente**	Monitoramento e revisão de serviços de fornecedores não documentados
5.23	Segurança da Informação para Uso de Serviços em Nuvem	**Controle** Processos para aquisição, uso, gerenciamento e saída de serviços em nuvem devem ser estabelecidos de acordo com os requisitos de Segurança da Informação da organização.	**Atende**	Políticas de segurança para serviços em nuvem documentadas e implementadas.
5.24	Preparação e Planejamento de Gerenciamento de Incidentes de Segurança da Informação	**Controle** A organização deve planejar-se e preparar-se para o gerenciamento de incidentes de Segurança da Informação, por meio da definição, do estabelecimento e da comunicação dos processos, funções e responsabilidades relativos a eles.	**Atende**	Planos de resposta a incidentes documentados e testados regularmente.
5.25	Avaliação e Decisão sobre Eventos de Segurança da Informação	**Controle** A organização deve avaliar os eventos de Segurança da Informação e	**Atende**	Procedimentos documentados para

		decidir se os categoriza como incidentes.		avaliação de eventos de segurança.
5.26	Resposta aos Incidentes de Segurança da Informação	**Controle** Incidentes de Segurança da Informação devem ser respondidos de acordo com os procedimentos documentados.	**Atende**	Procedimentos de resposta a incidentes documentados e aplicados.
5.27	Aprendizado com Incidentes de Segurança da Informação	**Controle** O conhecimento obtido a partir dos incidentes de Segurança da Informação deve ser usado a fim de fortalecer e melhorar seus controles.	**Atende**	Relatórios de lições aprendidas armazenados e revisados.
5.28	Coleta de Evidências	**Controle** A organização deve estabelecer e implementar procedimentos para a identificação, coleta, aquisição e preservação de evidências relacionadas aos eventos de Segurança da Informação.	**Atende**	Procedimentos documentados e seguidos para coleta de evidências.
5.29	Segurança da Informação durante Interrupção	**Controle** A organização deve planejar como manter um nível adequado de Segurança da Informação durante uma interrupção.	**Atende**	Planos de continuidade documentados e testados.
5.30	Disponibilidade de TIC para a Continuidade do Negócio	**Controle** A disponibilidade de TIC deve ser planejada, implementada, mantida e testada, baseada nos objetivos de negócio e requisitos de TIC para a continuidade.	**Atende**	Recursos TIC redundantes documentados e monitorados.

5.31	Requisitos Legais, Estatutários, Regulatórios e Contratuais	**Controle** Os requisitos legais, estatutários, regulatórios e contratuais relevantes para a Segurança da Informação e a abordagem organizacional para atender a esses requisitos devem passar por identificação, documentação e atualização constante.	**Atende**	Requisitos documentados e revisados periodicamente.
5.32	Direitos de Propriedade Intelectual	**Controle** A organização deve implementar procedimentos adequados para proteger direitos de propriedade intelectual.	**Atende**	Procedimentos documentados para proteção de propriedade intelectual.
5.33	Proteção de Registros	**Controle** Registros devem possuir proteção contra perda, destruição, falsificação e acesso e liberação não autorizados.	**Atende**	Políticas de proteção de registros documentadas e aplicadas.
5.34	Privacidade e Proteção de Informações de Identificação Pessoal (IIP)	**Controle** A organização deve identificar e atender aos requisitos a respeito da preservação da privacidade e proteção de IIP, de acordo com leis e regulações aplicáveis e requisitos contratuais.	**Atende**	Políticas de proteção de IIP documentadas e comunicadas.
5.35	Revisão Independente de Segurança da Informação	**Controle** A abordagem organizacional para o gerenciamento de Segurança da Informação e sua implementação, incluindo pessoas, processos e tecnologia, deve admitir revisão de forma independente em intervalos planejados, ou no momento em que mudanças significativas ocorrerem.	**Atende**	Auditorias independentes realizadas e documentadas.

5.36	Conformidade com Políticas, Regras e Padrões de Segurança da Informação	**Controle** Conformidade com Política de Segurança da Informação organizacional, políticas de tópicos específicos, regras e padrões devem passar regularmente por revisão.	**Atende**	Procedimentos de conformidade documentados e revisados.
5.37	Procedimentos Operacionais Documentados	**Controle** Procedimentos operacionais para recursos de processamento de informações devem ser documentados e deixados disponíveis aos colaboradores que os necessitem.	**Atende**	Procedimentos operacionais documentados e armazenados em PDF.
6	**Controles de Pessoas**		**Requisito**	**Evidência**
6.1	Seleção	**Controle** Os antecedentes de todos os colaboradores devem passar por verificação antes de ingressar na organização de forma contínua, conforme leis, regulamentos aplicáveis e ética, de maneira proporcional aos requisitos do negócio, à classificação das informações acessadas e aos riscos percebidos.	**Atende**	Realizado pelo time de RH através de sistemas internos da empresa.
6.2	Termos e Condições de Contratação	**Controle** Os acordos contratuais de trabalho devem indicar as responsabilidades dos colaboradores e da organização com a Segurança da Informação.	**Atende**	Incluídos nos contratos de trabalho e armazenados em PDF.
6.3	Treinamento, Educação e Conscientização em Segurança da Informação	**Controle** Colaboradores e partes interessadas relevantes devem receber conscientização sobre Segurança da Informação, educação,	**Atende**	Programas de treinamento regulares realizados por meio de *software.*

		treinamento e atualizações da Política de Segurança da Informação, bem como políticas de tópicos específicos e procedimentos, relevantes para as suas funções.		
6.4	Processo Disciplinar	**Controle** Um processo disciplinar deve ser formalizado e comunicado, a fim de tomar ações contra colaboradores e partes interessadas relevantes que tenham cometido violações na Política de Segurança da Informação.	**Atende**	Procedimentos documentados e aplicados, registrados em sistemas internos.
6.5	Responsabilidades após Término ou Mudança de Contratação	**Controle** Responsabilidades e obrigações de Segurança da Informação que permanecem válidas após término ou mudança da contratação devem ser definidas, aplicadas e comunicadas aos colaboradores e outras partes interessadas relevantes.	**Atende**	Procedimentos claros seguidos pelo RH e TI, documentados em PDF.
6.6	Acordos de Confidencialidade ou Não Divulgação	**Controle** Acordos de confidencialidade ou não divulgação que refletem as necessidades organizacionais para a proteção da informação devem passar por identificação, documentação, revisão regular e assinatura pelos colaboradores e outras partes interessadas relevantes.	**Atende**	Incluídos nos contratos de trabalho e armazenados em PDF.
6.7	Trabalho Remoto	**Controle** Medidas de segurança devem ser implementadas quando os colaboradores estão trabalhando remotamente, a fim de proteger as informações acessadas, processadas ou armazenadas fora das instalações da organização.	**Atende Parcialmente**	Medidas implementadas, mas com dificuldade de monitoramento

6.8	Relatórios de Eventos de Segurança da Informação	**Controle** A organização deve prover um mecanismo para os colaboradores reportarem eventos de Segurança da Informação observados ou suspeitos por meio de canais adequados, de maneira oportuna.	**Atende**	Registrado internamente e disponibilizado através de *dashboard.*
7	**Controles Físicos**		**Requisito**	**Evidência**
7.1	Perímetros de Segurança Física	**Controle** Perímetros de segurança devem ser definidos e usados, a fim de proteger áreas que contêm informações e outros ativos associados.	**Atende**	Documentação e mapas de segurança em PDF, armazenados internamente.
7.2	Entrada Física	**Controle** Áreas de segurança devem possuir proteção por controles de entrada apropriados e pontos de acesso.	**Atende**	Sistema de controle de acesso físico, registrado através de cartão de acesso.
7.3	Proteção de Escritórios, Salas e Instalações	**Controle** Segurança física para escritórios, salas e instalações deve ser projetada e implementada.	**Atende**	Políticas e procedimentos documentados e disponíveis em PDF.
7.4	Monitoramento de Segurança Física	**Controle** Instalações devem passar por monitoramento contínuo contra acesso físico não autorizado.	**Atende**	Sistemas de monitoramento físico implementados e geridos pela segurança local.

7.5	Proteção contra Ameaças Físicas e Ambientais	**Controle** Proteção contra ameaças físicas e ambientais, a saber, desastres naturais e outras ameaças físicas intencionais e não intencionais para a infraestrutura, devem ser projetadas e implementadas.	**Atende**	Procedimentos documentados.
7.6	Trabalho em Áreas Seguras	**Controle** Medidas de segurança para o trabalho em áreas seguras devem ser projetadas e implementadas.	**Atende**	Procedimentos documentados e acessíveis em sistemas internos.
7.7	Mesa e Tela Limpas	**Controle** Regras claras de mesa para papéis e mídias de armazenamento removíveis e regras claras de tela para recursos de processamento de informações devem passar por definição e aplicação adequadas.	**Atende**	Políticas documentadas e comunicadas, disponíveis em PDF.
7.8	Localização e Proteção de Equipamentos	**Controle** Equipamento deve estar em segurança e protegido.	**Atende**	Procedimentos documentados e monitorados através de *software*.
7.9	Segurança de Ativos Fora do Local	**Controle** Ativos externos devem ser protegidos.	**Atende Parcialmente**	Procedimentos de segurança documentados, mas difíceis de serem acompanhados e controlados.

7.10	Mídia de Armazenamento	**Controle** A mídia de armazenamento deve admitir gerenciamento por meio do ciclo de vida de aquisição, uso, transporte e descarte, de acordo com o esquema de classificação e requisitos de manuseio da organização.	**Atende**	Gestão de mídias removíveis documentadas e implementadas.
7.11	Utilitários de Suporte	**Controle** Os recursos de processamento de informações devem possuir proteção contra falhas de energia e outras interrupções causadas por erros no suporte.	**Atende**	Controles documentados e verificados regularmente.
7.12	Segurança de Cabeamento	**Controle** Os cabos que transportam energia, dados ou serviços de informação de apoio devem possuir proteção contra interceptação, interferência ou danos.	**Atende**	Políticas documentadas em PDF e verificações periódicas registradas.
7.13	Manutenção de Equipamento	**Controle** Os equipamentos devem ser mantidos corretamente, a fim de garantir disponibilidade, integridade e confidencialidade das informações.	**Atende**	Manutenção feita de forma recorrente e registros de manutenção armazenados em *software*.
7.14	Descarte ou Reutilização Segura de Equipamento	**Controle** Os itens do equipamento que contêm mídia de armazenamento devem ser verificados para garantir que quaisquer dados sensíveis e *softwares* licenciados foram removidos ou substituídos com segurança antes de	**Atende**	Procedimentos de eliminação feitos de forma segura e documentados e registrados em

		serem descartados ou reutilizados.		*software*.
8	**Controles Tecnológicos**		**Requisito**	**Evidência**
8.1	Dispositivos *Endpoint* do Usuário	**Controle** Informações armazenadas, processadas ou acessíveis por meio de dispositivos *endpoint* de usuários devem ser protegidas.	**Atende**	Implementado e monitorado através de *software* de gestão de dispositivos.
8.2	Direitos de Acesso Privilegiados	**Controle** A atribuição e a utilização de direitos de acesso privilegiados devem ser restringidas e geridas.	**Atende**	Políticas de acesso privilegiado documentadas e controladas via sistema.
8.3	Restrição de Acesso à Informação	**Controle** Acesso à informação e outros ativos associados devem ser restringidos de acordo com as políticas de tópicos específicos estabelecidas no controle de acesso.	**Atende**	Políticas de acesso documentadas e monitoradas através de *software* de segurança.
8.4	Acesso ao Código-Fonte	**Controle** Acesso de leitura e escrita ao código-fonte, ferramentas de desenvolvimento e bibliotecas de *software* devem ser adequadamente gerenciadas.	**Atende**	Controle de acesso ao código-fonte implementado e registrado em sistemas internos, acessível apenas a usuários com acesso permitido.

8.5	Autenticação Segura	**Controle** Tecnologias e procedimentos de autenticação segura devem ser implementados baseados em restrições a informações e política de tópicos específicos sobre controle de acesso.	**Atende**	Implementação de autenticação multifator documentada e monitorada.
8.6	Gerenciamento de Capacidade	**Controle** A utilização dos recursos deve ser monitorada e ajustada de acordo com os requisitos de capacidade atuais e esperados.	**Atende**	Relatórios de capacidade gerados e revisados regularmente.
8.7	Proteção contra *Malware*	**Controle** A proteção contra *malware* deve ser implementada e suportada pela conscientização adequada do usuário.	**Atende**	*Software* antivírus e anti-*malware* implementados e monitorados.
8.8	Gerenciamento de Vulnerabilidades Técnicas	**Controle** Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas e a exposição da organização a tais vulnerabilidades deve ser avaliada, tomando medidas adequadas.	**Atende**	Ferramentas de escaneamento de vulnerabilidades gerenciamento e monitoramento de relatórios
8.9	Gerenciamento de Configuração	**Controle** Configurações, incluindo as de segurança, *hardware*, *software*, serviços e redes, devem ser estabelecidas, documentadas, implementadas, monitoradas e revisadas.	**Atende**	Configurações documentadas e gerenciadas via *software* de configuração.

8.10	Exclusão de Informações	**Controle** Informações armazenadas em sistemas de informação, dispositivos ou em qualquer outra mídia de armazenamento devem ser excluídas no momento em que não forem mais necessárias.	**Atende**	Procedimentos de exclusão de informações documentadas e monitoradas.
8.11	Mascaramento de Dados	**Controle** Mascaramento de dados deve ser utilizado de acordo com políticas de tópicos específicos de controle de acesso e outros relacionados, bem como requisitos de negócio, levando em consideração a legislação aplicável.	**Atende**	Técnicas de mascaramento de dados implementadas e documentadas.
8.12	Prevenção de Vazamento de Dados	**Controle** Medidas de prevenção de vazamento de dados devem ser aplicadas a sistemas, redes e quaisquer outros dispositivos que processem, armazenem ou transmitam informações sensíveis.	**Atende**	Ferramentas de DLP, acompanhamento e monitoramento implementadas.
8.13	*Backup* de Informações	**Controle** Cópias de segurança da informações, *software* e sistemas devem ser mantidas e testadas regularmente, de acordo com a política de tópicos específicos de *backup*.	**Atende Parcialmente**	Planos de *backup* testados regularmente, mas documentação descentralizada.
8.14	Redundância de Recursos de Processamento de Informações	**Controle** Recursos de processamento de informações devem ser implementados com redundância suficiente, a fim de atender aos requisitos de disponibilidade.	**Atende Parcialmente**	Presente, mas não documentado.

8.15	Registro de *Logs*	**Controle** *Logs* que registram atividades, exceções, falhas e outros eventos relevantes devem ser produzidos, armazenados, protegidos e analisados.	**Atende**	Logs armazenados e monitorados via *software* de gestão de logs.
8.16	Atividades de Monitoramento	**Controle** Redes, sistemas e aplicações devem ser monitorados em razão de comportamento anômalo e ações apropriadas devem ser tomadas a fim de avaliar potenciais incidentes de Segurança da Informação.	**Atende**	Monitoramento contínuo documentado e realizado via ferramentas de monitoramento.
8.17	Sincronização de Relógio	**Controle** Os relógios dos sistemas de processamento de informações utilizados pela organização devem estar sincronizados.	**Atende**	Relógios sincronizados via NTP e monitorados regularmente.
8.18	Uso de Programas Utilitários Privilegiados	**Controle** O uso de programas utilitários que possam substituir os controles de sistema e aplicativos deve ser restringido e rigidamente controlado.	**Não Atende**	Ausente
8.19	Instalação de *Software* em Sistemas Operacionais	**Controle** Procedimentos e medidas devem ser implementados, a fim de gerenciar de maneira segura a instalação de *software* em sistemas operacionais.	**Atende**	Políticas de instalação de software documentadas, mas há folgas no monitoramento e no controle dos *software* instalados.

8.20	Segurança de Redes	**Controle** Redes e seus dispositivos devem ser protegidos, gerenciados e controlados, a fim de salvaguardar as informações em sistemas e aplicações.	**Atende**	*Firewalls* e VPNs implementados e monitorados.
8.21	Segurança de Serviços de Rede	**Controle** Mecanismos de segurança, níveis de serviço e requisitos de serviço de rede devem ser identificados, implementados e monitorados.	**Atende**	Políticas de segurança de serviços de rede documentadas e implementadas.
8.22	Segregação de Redes	**Controle** Grupos de serviços de informações, usuários e sistemas de informação devem ser segregados nas redes da organização.	**Atende**	Redes segregadas conforme políticas documentadas.
8.23	Filtragem da *Web*	**Controle** O acesso a sites externos deve ser gerenciado, a fim de reduzir a exposição a conteúdos maliciosos.	**Atende**	Sistemas de prevenção de *malware* para impedir o acesso a recursos não autorizados presente.
8.24	Uso de Criptografia	**Controle** Regras para o uso eficaz da criptografia, incluindo o gerenciamento de chaves criptográficas, devem ser definidas e implementadas.	**Atende**	Criptografia aplicada a dados em trânsito e em repouso, monitorada.
8.25	Ciclo de Vida de Desenvolvimento Seguro	**Controle** Regras para o desenvolvimento seguro de *software* e sistemas devem ser estabelecidas e aplicadas.	**Atende**	Procedimentos documentados e seguidos durante o

				desenvolvimento.
8.26	Requisitos de Segurança de Aplicações	**Controle** Requisitos de Segurança da Informação devem ser identificados, especificados e aprovados durante o desenvolvimento ou aquisição de aplicações.	**Atende**	Documentação de requisitos armazenada em sistemas internos.
8.27	Princípios de Arquitetura e Engenharia em Sistemas Seguros	**Controle** Princípios para engenharia em sistemas seguros devem ser estabelecidos, documentados, mantidos e aplicados a quaisquer atividades de desenvolvimento de sistemas de informação.	**Atende**	Princípios documentados e seguidos durante o desenvolvimento.
8.28	Codificação Segura	**Controle** Princípios de codificação segura devem ser aplicados ao desenvolvimento de *software*.	**Atende**	Práticas de codificação segura implementadas e monitoradas.
8.29	Testes de Segurança em Desenvolvimento e Aceitação	**Controle** Processos de teste de segurança devem ser definidos e implementados no ciclo de vida de desenvolvimento.	**Atende**	Testes documentados e realizados regularmente.
8.30	Desenvolvimento Terceirizado	**Controle** A organização deve dirigir, monitorar e revisar as atividades relacionadas à terceirização de desenvolvimento de sistemas.	**Atende**	Políticas de segurança documentadas para desenvolvimento terceirizado.
8.31	Separação de Ambientes de Desenvolvimento, Teste e	**Controle** Os ambientes de desenvolvimento, teste e produção devem ser	**Atende**	Ambientes segregados conforme políticas documentadas.

	Produção	separados e protegidos.		
8.32	Gerenciamento de Mudanças	**Controle** Mudanças nos recursos de processamento de informações e nos sistemas devem estar sujeitas a alterações nos procedimentos de gerenciamento.	**Atende**	Mudanças controladas e registradas via *software* de gestão.
8.33	Informações de Teste	**Controle** Informações de teste devem ser adequadamente selecionadas, protegidas e gerenciadas.	**Atende**	Dados de teste documentados e gerenciados conforme políticas.
8.34	Proteção de Sistemas de Informação durante Testes de Auditoria	**Controle** Os testes de auditoria e outras atividades de garantia que envolvam avaliação de sistemas operacionais devem ser planejados e acordados entre os testadores e a gerência.	**Atende**	Procedimentos documentados e seguidos durante auditorias.

Fonte: Adaptado da ISO 27002:2022

4.2. Análise dos Pontos Fortes e Fracos

Neste tópico, apresentaremos os pontos fortes e fracos identificados na análise de aderência aos controles da ISO/IEC 27001. Vale ressaltar que para o diagnóstico foi considerado "Atende" para a existência dos controles e "Atende Parcialmente" para a existência parcial dos controles, e "Não Atende" para a ausência dos controles, já para evidência foram considerados documentos fornecidos, sistemas ou *software* mencionado nas entrevistas ou coletados durante a busca de dados. Foram compiladas as principais informações sobre os pontos fortes e fracos da implementação.

Sobre os pontos fortes (ver Quadro 9) refletem o comprometimento da organização com a implementação de controles essenciais para a segurança da informação. Entre os destaques, estão as políticas para segurança da informação, que se encontram bem estabelecidas e documentadas. A existência de arquivos em PDF, disponíveis em sistemas internamente, facilita a comunicação e compreensão das políticas entre os colaboradores. Esse tipo de documentação assegura que todos compreendam as diretrizes a serem seguidas, promovendo um ambiente de trabalho alinhado às boas práticas.

> *"(...) vai depender muito também do escopo, porque, por exemplo, na política de segurança, temos Brasil, México e Colômbia com três políticas distintas. Hoje, temos uma política global, mas o processo de revisão e atualização dessas políticas não ocorre de forma conjunta. É tipo, chegou a hora de revisar a política da empresa, e cada uma vai sendo revisada de acordo com o seu tempo."* (E3)

Outro aspecto positivo está relacionado à definição de papéis e responsabilidades de segurança. A clareza na atribuição dessas funções garante que cada colaborador saiba exatamente suas responsabilidades no que tange à proteção da informação, reduzindo ambiguidades e prevenindo falhas decorrentes de falta de governança. Esse controle é reforçado por um processo estruturado de segregação de funções, que minimiza riscos ao garantir que atividades críticas sejam realizadas por pessoas ou equipes distintas.

> *"(...) a gente usa um monte de ferramentas para gerenciar nossas documentações e treinamentos internos, além de outras ferramentas para as tarefas do dia a dia. Por exemplo, todas as nossas documentações internas ficam armazenadas no Confluence, o que facilita o acesso e a colaboração entre os membros da equipe. Os treinamentos, por sua vez, são feitos no Deegred, uma plataforma que nos ajuda a organizar e acompanhar o progresso dos programas de capacitação. No nosso dia a dia, usamos várias outras ferramentas para apoiar os diferentes times. O Jira*

> *é utilizado para gerenciamento de projetos e acompanhamento de tarefas, o Slack para comunicação instantânea e integração das equipes, e o GitHub para versionamento e controle de código, com acesso controlado. Além disso, temos vários comitês mensais entre os times para discutir os principais riscos da companhia, que são escalados conforme necessário para que a gente possa tomar um plano de ação (...)"* (E4)

Além disso, a organização demonstra maturidade ao manter um sistema estruturado de contato com autoridades. Essa prática, sustentada por registros documentados e centralizados, assegura que, em situações de crise ou incidentes de segurança, a comunicação com entidades externas ocorra de forma eficiente e alinhada às exigências legais. Por fim, as responsabilidades de gestão estão bem descritas nas políticas internas, o que reflete um compromisso claro da alta administração com a segurança da informação, promovendo uma cultura de responsabilidade.

Quadro 9: Pontos Fortes

Pontos Fortes	
Comprometimento da alta liderança	A alta gestão está comprometida com a segurança da informação, com responsabilidades bem definidas e claramente documentadas em políticas internas. Isso garante que a governança esteja alinhada às melhores práticas e as decisões de segurança sejam tomadas de forma consistente.
Processos robustos	A organização tem processos bem estruturados, como as políticas de segurança e a segregação de funções, que estão formalmente documentadas e seguidas. Isso promove a segurança da informação e a prevenção de falhas operacionais.
Treinamento e Conscientização	Programas contínuos de conscientização e treinamento em segurança da informação para todos os funcionários.
Auditorias Internas	Realização regular de auditorias internas para avaliar a eficácia do SGSI.
Documentação centralizada e acessível	A documentação sobre políticas e responsabilidades está centralizada e acessível em formatos como PDF, o que facilita a consulta e garante que todos os colaboradores tenham acesso às informações necessárias para seguir as normas de segurança.

Fonte: Autoria própria

Grande parte das informações já foram ou estão sendo implementadas, o que demonstra um grande comprometimento da empresa em conseguir garantir as boas práticas

presentes na ISO 27002, isso pode ser evidenciado durante as entrevistas, principalmente entre a alta liderança.

> *"Assim, de fato, você vai encontrar muitas informações. Se você pegar os requisitos, consegue identificar rapidamente o que está presente e o que falta. Por exemplo, há requisitos para educação e treinamento, revisão técnica, aplicação de mudanças no sistema e gestão de mudanças. As políticas também estão incluídas. Estou verificando os requisitos da ISO e podemos ver que muitos desses elementos já estão implementados aqui."* (E2)

Por outro lado, os pontos fracos (ver Quadro 10) destacam desafios significativos, sendo que a principal dificuldade da empresa hoje está na documentação dos controles. Embora muitos processos estejam sendo executados, a ausência de registros formais prejudica a rastreabilidade e a comprovação de conformidade. Esse problema é particularmente evidenciado durante as entrevistas e o diagnóstico dos controles como o contato com grupos de interesses especiais, onde faltam evidências documentadas que demonstrem esforços para engajamento com associações do setor ou iniciativas colaborativas.

> *"Documentação de processos a gente é ruim nisso, a gente faz muita coisa, mas a gente é péssimo para documentar e é uma coisa que o time tá trabalhando agora."* (E3)

Outro exemplo crítico é a falta de um processo estruturado para inteligência contra ameaças. Sem práticas documentadas que permitam monitorar e responder a ameaças emergentes, a organização permanece vulnerável a riscos cibernéticos crescentes. A inexistência de um inventário de informações e ativos associados também é um ponto fraco importante, pois dificulta a identificação, proteção e gestão desses ativos, comprometendo a integridade e disponibilidade das informações. A ausência de políticas formalizadas para o uso de programas utilitários privilegiados representa outra lacuna que exige atenção. Sem regulamentações claras e documentadas, há riscos associados a acessos não autorizados ou uso indevido de privilégios administrativos.

Os controles parcialmente implementados demonstram um esforço inicial positivo, mas precisam de maior detalhamento e padronização. Por exemplo, o gerenciamento de segurança na cadeia de suprimentos apresenta processos básicos documentados, mas carece de integração e supervisão mais rigorosa dos fornecedores. O monitoramento, revisão e gerenciamento de mudanças, embora presente, são realizados de forma inconsistente, o que pode gerar vulnerabilidades durante transições tecnológicas ou organizacionais.

A segurança de ativos fora do local durante o trabalho remoto e os backups de informações também são áreas que necessitam de melhoria na documentação. Apesar de existirem práticas em andamento, a ausência de registros formais dificulta a comprovação de conformidade e a validação dos processos.

> *"Por exemplo, não tem política de Backup Centralizado dentro do empresa, então a gente não consegue atender esse tópico (...)"* (E2)

No caso da redundância de recursos de processamento de informações, a implementação é aparente, mas a falta de evidências documentadas impede que se confirme a adequação do controle às exigências da ISO 27001.

Esses desafios evidenciam que, embora a organização tenha avançado significativamente na execução de muitos controles, a deficiência na documentação formal é um obstáculo central. Sem essa documentação, não apenas a conformidade com a norma é comprometida, mas também a capacidade de monitorar, revisar e aprimorar continuamente os processos. Para superar essas lacunas, é essencial priorizar a formalização de evidências, criar mecanismos de registro consistentes e assegurar que todos os controles sejam adequadamente documentados. Isso permitirá não apenas a conformidade com a norma, mas também uma postura mais sólida e resiliente frente a riscos e auditorias.

Quadro 10: Pontos Fracos

Pontos Fracos	
Documentação	Em vários controles, como o contato com grupos de interesses especiais e o uso de programas utilitários privilegiados, há uma ausência de documentação formal. Isso dificulta a comprovação da conformidade e deixa lacunas no controle de processos críticos.
Detalhamento nos processos	O gerenciamento de segurança na cadeia de suprimentos e o monitoramento e gerenciamento de mudanças possuem processos, mas com detalhamento insuficiente. Isso pode gerar falhas na execução desses controles, impactando a segurança da organização de forma negativa.
Planejamento para revisão dos processos	No caso de alguns controles como a segurança de ativos fora do local e os backups de informações, a falta de documentação e revisão adequadas sugere que a organização não tem tempo suficiente ou um planejamento adequado

	para garantir que esses processos sejam bem executados e acompanhados.
Gestão de acesso fora do local de trabalho	A empresa não possui um controle rigoroso de acesso que garanta que apenas indivíduos autorizados tenham acesso a informações sensíveis fora do local de trabalho.

Fonte: Autoria própria

Essas questões ainda não foram estabelecidas dentro da companhia, o que gera um desconforto diante da alta liderança.

> *"(...) acho que a questão não é apenas fazer essa avaliação. A grande questão pode estar em compartilhar informações sensíveis. Por exemplo, existem processos e requisitos de gestão de acesso que, ao serem apontados como ausentes, podem causar estranheza. Isso pode, de certa forma, gerar preocupação."* (E1)

A análise dos pontos fortes e fracos da implementação dos controles da ISO/IEC 27002 revela uma postura robusta em segurança da informação, com 89% de conformidade. Observa-se uma preocupação significativa por parte da liderança em alcançar 100% de conformidade. A equipe já está alinhada com diversos aspectos dos requisitos, além de contar com processos robustos e um gerenciamento de riscos eficaz.

No entanto, há áreas críticas que necessitam de melhorias. A falta de documentação formal em controles importantes pode comprometer a rastreabilidade e a conformidade com as melhores práticas de segurança. Além disso, a falta de implementação estruturada expõe a organização a riscos cibernéticos e dificulta o controle adequado de ativos críticos.

Além disso, a falta de tempo e planejamento adequados para revisar processos indica que esses controles podem não estar sendo totalmente otimizados ou documentados, o que representa uma vulnerabilidade para a organização.

Em resumo, embora a empresa apresente um forte comprometimento da alta liderança e tenha processos robustos em muitas áreas, abordando as falhas nas documentações e implementações estruturadas, poderá fortalecer ainda mais sua postura de segurança e reduzir significativamente os riscos residuais. A organização já possui uma base sólida, mas a padronização e o detalhamento adicional de alguns processos críticos são essenciais para garantir a conformidade total e minimizar as vulnerabilidades identificadas.

4.3. Análise das Lacunas em Relação às Normas ISOs

A análise das lacunas em relação à conformidade com as normas ISO/IEC 27001 e ISO/IEC 27002 identificou 10 controles (4 Não Atendem e 6 Atendem Parcialmente) que precisam ser priorizados para alcançar 100% de conformidade. As principais lacunas encontradas são as seguintes (Quadro 11):

Quadro 11: Lacunas em relação à norma ISO 27001:2022

Tipo de Controle	ID do Controle	Propósito do Controle	Requisito	Evidência
Organizacional	5.6	Assegurar que a troca de informações ocorra de maneira adequada, respeitando os princípios de Segurança da Informação.	**Não Atende**	Ausente
Organizacional	5.7	Fornecer conhecimento sobre o ambiente de ameaças da organização para a tomada de ações de mitigação apropriadas.	**Não Atende**	Ausente
Organizacional	5.9	Garantir que todos os ativos de informação e associados sejam identificados, registrados e protegidos de forma adequada para minimizar riscos à segurança.	**Não Atende**	Ausente
Organizacional	5.21	Preservar o nível estabelecido de Segurança da Informação nas relações com fornecedores.	**Atende Parcialmente**	Procedimentos de gestão de segurança da cadeia de suprimentos de TIC não documentados.
Organizacional	5.22	Garantir a conformidade com os contratos de fornecedores, mantendo o	**Atende Parcialmente**	Monitoramento e revisão de serviços de fornecedores não documentados

		nível de Segurança da Informação e a qualidade dos serviços acordados.		
Pessoas	6.7	Estabelecer políticas e controles para garantir que a segurança da informação seja mantida, mesmo quando os colaboradores estiverem trabalhando fora das instalações da empresa.	**Atende Parcialmente**	Medidas implementadas, mas com dificuldade de monitoramento
Físicos	7.9	Impedir a perda, dano ou roubo de dispositivos externos e evitar interrupções nas operações da organização.	**Atende Parcialmente**	Procedimentos de segurança documentados, mas difíceis de serem acompanhados e controlados.
Tecnológicos	8.13	Assegurar que cópias de segurança das informações críticas sejam realizadas regularmente e armazenadas de forma segura, garantindo a recuperação dos dados em caso de falha ou incidente.	**Atende Parcialmente**	Planos de *backup* testados regularmente, mas documentação descentralizada.
Tecnológicos	8.14	Assegurar a operação ininterrupta dos recursos de processamento de dados.	**Atende Parcialmente**	Presente, mas não documentado.
Tecnológicos	8.18	Assegurar que o uso de programas utilitários não comprometa os controles de sistemas e aplicativos relacionados à Segurança da Informação.	**Não Atende**	Ausente

Fonte: Autoria própria

Para alcançar a conformidade total com as normas ISO/IEC 27001 e ISO/IEC 27002, é essencial que a empresa priorize a implementação dos controles mencionados. Para isso, foi necessário alinhar as recomendações com base no diagnóstico. Dessa forma, poderão ser tomadas as medidas necessárias para resolvê-los.

5. PROPOSTA DE MELHORIA

Neste tópico, vamos abordar a proposta de melhoria para implementar controles de segurança da informação, utilizando o 5W+1H. Esta abordagem visa aprimorar a segurança e a eficácia dos processos de gestão de riscos dentro da organização, garantindo a conformidade e a proteção das informações sensíveis. A proposta detalhará as ações necessárias para atender aos requisitos de segurança identificados, melhorar a infraestrutura existente e mitigar possíveis vulnerabilidades, assegurando a continuidade e a integridade das operações.

5.1. Recomendações Baseadas no Diagnóstico

Com base no diagnóstico realizado, as seguintes recomendações são baseadas no 5W+1H (ver Quadro 12) para aprimorar a segurança da informação na organização. Este processo contou com a colaboração dos gerentes de segurança da informação e risco de TI, garantindo que as sugestões estejam alinhadas com as práticas de gestão de riscos e segurança da informação. As recomendações focam na implementação de controles específicos para mitigar vulnerabilidades identificadas, fortalecer a infraestrutura de segurança existente e promover uma cultura de conscientização sobre a importância da segurança da informação entre todos os colaboradores.

Quadro 12: Recomendações para as Lacunas

Tipo de Controle	**ID do Controle**	**Controle**	**Requisito**	*What*	*Why*	*Who*	*When*	*Where*	*How*	*Status*
Organizacional	5.6	Contato com Grupos de Interesses Especiais	**Não Atende**	Estabelecer contato com grupos de interesse especializados	Obter informações sobre ameaças e melhores práticas	Equipe de Segurança da Informação	Para o 2º Sem. de 2025	Empresa como um todo	Documentação, treinamentos, comitês ou fóruns	Pendente
Organizacional	5.7	Inteligência contra Ameaças	**Não Atende**	Implementar um sistema de inteligência contra ameaças	Identificar e mitigar ameaças em tempo real	Equipe de Segurança da Informação e Engenharia	Para o 1º Sem. e 2º Sem. de 2025	Empresa como um todo	Parcerias com fornecedores de inteligência contra ameaças ou desenvolver internamente.	Pendente
Organizacional	5.9	Inventário de Informações e outros Ativos Associados	**Não Atende**	Criar e manter um inventário atualizado de informações e ativos	Garantir a visibilidade e controle sobre os ativos da organização	Equipe de TI e Segurança da Informação	Para o 1º Sem. e 2º Sem. de 2025	Empresa como um todo	Ferramentas de gerenciamento de ativos e auditorias regulares	Pendente
Organizacional	5.21	Gerenciamento de Segurança da	**Atende Parcialmente**	Estabelecer um processo de	Garantir a segurança em	Gestores de Suprimentos e	Para o 1º Sem. de 2025	Todos os fornecedore	Contratos de serviço com	Em Progresso

		Informação na Cadeia de Suprimentos de Tecnologia da Informação e Comunicação (TIC)		gerenciamento de segurança na cadeia de suprimentos	todos os níveis da cadeia de suprimentos	Segurança		s de TIC	cláusulas de segurança	
Organizacional	5.22	Monitoramento, Revisão e Gerenciamento de Mudanças de Serviços de Fornecedores	**Atende Parcialmente**	Implementar processos de monitoramento e revisão de mudanças	Manter a segurança e a integridade dos serviços de fornecedores	Gestores de Suprimentos e Segurança	Para o 1º Sem. de 2025	Todos os fornecedores de TIC	Auditorias regulares e avaliações de risco	Em Progresso
Pessoas	6.7	Trabalho Remoto	**Atende Parcialmente**	Estabelecer controles de segurança para trabalho remoto	Assegurar a proteção de informações e sistemas acessados remotamente	RH, TI e Equipe de Segurança da Informação	Para o 1º Tri. de 2025	Locais externos e remotos	Treinamentos e ferramentas de acesso seguro	Em Validação
Físicos	7.9	Segurança de Ativos Fora do Local	**Atende Parcialmente**	Estabelecer políticas de segurança para ativos fora do local	Proteger dados e equipamentos em locais remotos	Todos os colaboradores e Equipe de TI	Para o 1º Tri. de 2025	Locais externos e remotos	Políticas de segurança para dispositivos e de transporte seguro	Em Validação

Tecnológicos	8.13	Backup de Informações	**Atende Parcialmente**	Estabelecer e centralizar regularmente backups de informações críticas	Garantir a recuperação de dados em caso de perda	Equipe de TI	Para o 1º Tri. de 2025	Empresa como um todo	Políticas de backup, ferramentas de backup automatizadas e testes regulares	Em Progresso
Tecnológicos	8.14	Redundância de Recursos de Processamento de Informações	**Atende Parcialmente**	Estabelecer redundância de recursos de processamento	Garantir disponibilidade contínua de serviços	Equipe de TI e Engenharia	Para o 1º Sem. e 2º Sem. de 2025	Data Center	Implementação de sistemas redundantes e planos de contingência	Em Validação
Tecnológicos	8.18	Uso de Programas Utilitários Privilegiados	**Não Atende**	Controlar o uso de programas utilitários privilegiados	Evitar uso indevido de programas sensíveis	Equipe de TI e Segurança da Informação	Para o 1º Sem. e 2º Sem. de 2025	Sistemas internos	Ferramentas de gerenciamento de privilégios e auditorias	Pendente

Fonte: Autoria própria

Cada controle foi preenchido com base no método 5W+1H, alinhados em reunião tanto com o gerente de riscos de TI, quanto o gerente de segurança da informação, para fornecer uma visão clara e detalhada de como implementar cada requisito. Esta abordagem ajuda a definir claramente as ações necessárias, os motivos por trás dessas ações, quem será responsável, quando e onde as ações serão realizadas, e como serão implementadas.

5.2. Plano de Ação para Adequação às Normas ISO 27001 e ISO 27002

Para propor um Plano de Ação para adequação às normas ISO 27001 e ISO 27002 utilizando a estrutura do NIST, é essencial abordar as cinco funções principais do NIST: Identificar, Proteger, Detectar, Responder e Recuperar. A análise do gráfico mostra que a empresa possui uma visão bem definida em relação aos domínios, indicando um alinhamento entre os processos. Este é um ponto positivo para alcançar a conformidade de 100% no futuro. No entanto, é importante lembrar que a nota mínima exigida pela companhia é 3. Portanto, mesmo que a pontuação esteja próxima de 3, é fundamental buscar melhorias contínuas.

I. Identificar (*Identify*): Com uma percepção atual de 3,24 (InfoSec) e 3,07 (Outras BUs), o objetivo é melhorar a identificação e documentação de ativos e processos. As ações incluem mapear e catalogar ativos, implementar um sistema de gestão de ativos que documente todos os ativos de TI da empresa, realizar avaliações de risco regulares e documentar todas as descobertas e planos de mitigação, e desenvolver programas de treinamento para garantir que todos os colaboradores entendam a importância da identificação de ativos e riscos.
II. Proteger (*Protect*): Com uma percepção atual de 2,97 (InfoSec) e 2,87 (Outras BUs), o objetivo é fortalecer as medidas de proteção para assegurar a integridade e a confidencialidade dos dados. As ações incluem reforçar os controles de acesso, garantindo que apenas pessoal autorizado tenha acesso a informações sensíveis, implementar treinamentos regulares sobre segurança da informação para todos os funcionários, e desenvolver e manter atualizados os procedimentos de segurança, garantindo que sejam seguidos por todos.
III. Detectar (*Detect*): Com uma percepção atual de 3,67 (InfoSec) e 3,39 (Outras BUs), o objetivo é melhorar a capacidade de detectar ameaças e incidentes de segurança. As ações incluem implementar sistemas avançados de monitoramento e detecção de ameaças, realizar análises de logs e auditorias de segurança periodicamente, e

documentar e treinar equipes em procedimentos de resposta rápida a incidentes detectados.

IV. Responder (*Respond*): Com uma percepção atual de 3,94 (InfoSec) e 4,06 (Outras BUs), o objetivo é garantir uma resposta eficaz e eficiente a incidentes de segurança. As ações incluem desenvolver, documentar e testar planos de resposta a incidentes, treinar uma equipe dedicada à resposta a incidentes, garantindo que saibam seguir os procedimentos documentados, e estabelecer procedimentos claros de comunicação durante e após um incidente de segurança.

V. Recuperar (*Recover*): Com uma percepção atual de 3,17 (InfoSec) e 3,00 (Outras BUs), o objetivo é assegurar a recuperação rápida e eficaz após incidentes de segurança. As ações incluem desenvolver e testar regularmente planos de continuidade de negócios e recuperação de desastres, implementar uma política rigorosa de backups regulares e testes de restauração, e realizar avaliações pós-incidentes para identificar lições aprendidas e melhorar os processos de recuperação.

Com este plano de ação, a empresa pode melhorar significativamente sua conformidade com as normas ISO 27001 e ISO 27002, fortalecendo sua postura de segurança e minimizando riscos.

5.3. Medidas para Mitigação de Riscos

Para introduzir o tópico de medidas para mitigação de riscos, é essencial explicar a metodologia utilizada para avaliar e priorizar os riscos identificados. Foi utilizada uma matriz de impacto e probabilidade, alinhado com o gerente de riscos de TI que utilizou um sistema interno, alinhada com a metodologia interna da empresa, para definir o grau de impacto e probabilidade de cada controle, para identificar os principais problemas. A matriz classifica os riscos qualitativamente em termos de impacto (baixo, médio ou alto) e probabilidade (baixo, médio ou alto), permitindo uma visualização clara das áreas que requerem atenção prioritária. O Quadro 13 resume os controles que apresentam problemas, classificando-os de acordo com o seu impacto e sua probabilidade de ocorrência.

Quadro 13: Impacto e Probabilidade dos Principais Problemas

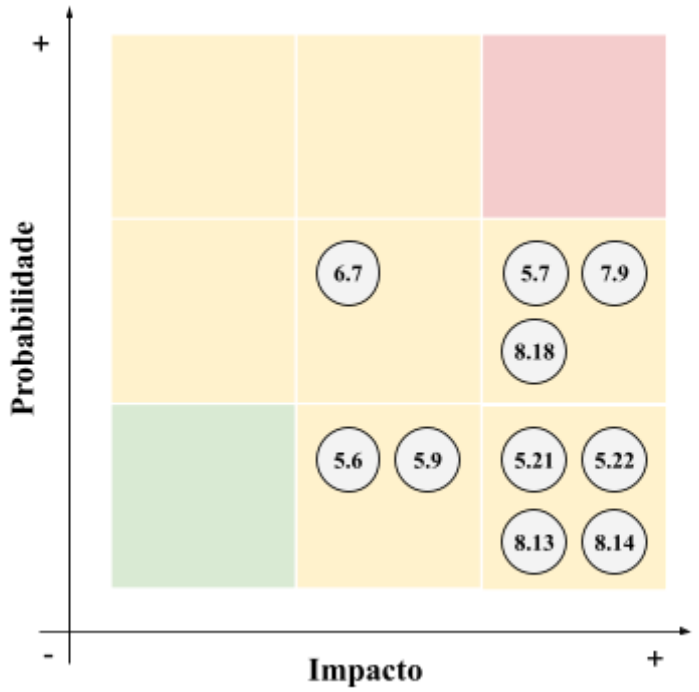
Tipo de	ID do Controle	Controle	Impacto	Probabilidade

Controle				
Organizacional	5.6	Contato com Grupos de Interesses Especiais	Médio	Baixo
Organizacional	5.7	Inteligência contra Ameaças	Alto	Médio
Organizacional	5.9	Inventário de Informações e outros Ativos Associados	Médio	Baixo
Organizacional	5.21	Gerenciamento de Segurança da Informação na Cadeia de Suprimentos de Tecnologia da Informação e Comunicação (TIC)	Alto	Baixo
Organizacional	5.22	Monitoramento, Revisão e Gerenciamento de Mudanças de Serviços de Fornecedores	Alto	Baixo
Pessoas	6.7	Trabalho Remoto	Médio	Médio
Físicos	7.9	Segurança de Ativos Fora do Local	Alto	Médio
Tecnológicos	8.13	Backup de Informações	Alto	Baixo
Tecnológicos	8.14	Redundância de Recursos de Processamento de Informações	Alto	Baixo
Tecnológicos	8.18	Uso de Programas Utilitários Privilegiados	Alto	Médio

Fonte: Autoria própria

A partir dessa análise, é possível desenvolver medidas específicas de mitigação para cada risco identificado, priorizando aqueles com maior impacto e probabilidade dentro da matriz (ver Figura 16).

Figura 16: Matriz de Probabilidade e Impacto dos Principais Problemas



Fonte: Autoria própria

6. CONCLUSÃO

Este trabalho focou na avaliação da conformidade de uma empresa de serviços financeiros com as normas ISO 27001 e ISO 27002, bem como na identificação das lacunas existentes nos processos de segurança da informação e na proposição de um plano de ação para alcançar 100% de conformidade.

A análise da empresa, com base na estrutura NIST e na avaliação das práticas de segurança de acordo com os domínios “Identificar”, “Proteger”, “Detectar”, “Responder” e “Recuperar”, revelou que a organização já possui uma visão clara e alinhada dos seus processos. No entanto, algumas áreas ainda apresentam oportunidades significativas de melhoria, particularmente nas categorias com as menores pontuações, como “Manutenção”, “Gestão de Riscos da Cadeia de Fornecedores”, “Processos e Procedimentos de Proteção” e “Gestão de Ativos”, que estão diretamente relacionadas à falta de documentação adequada e a processos mal definidos.

Além disso, ao identificar as lacunas com relação às normas ISO 27001 e ISO 27002 em áreas como “Inteligência contra Ameaças”, “Inventário de Informações e Ativos Associados”, e “Monitoramento de Fornecedores”, ficou claro que a empresa deve adotar medidas específicas para mitigar riscos nessas frentes.

Diante desse cenário, o plano de ação proposto busca, prioritariamente, fortalecer a documentação e os controles internos, além de aumentar a conscientização e o treinamento contínuo dos colaboradores. A implementação de medidas para melhorar o gerenciamento de fornecedores, a proteção dos ativos e a continuidade das operações são essenciais para garantir a segurança da informação e atender aos requisitos das normas ISO.

Portanto, com um plano de ação bem estruturado e a execução das melhorias necessárias, a empresa tem condições de alcançar 100% de conformidade com as normas ISO 27001 e ISO 27002, fortalecendo sua postura em segurança da informação e reduzindo riscos de forma significativa. O compromisso de toda a organização, especialmente da liderança, será fundamental para a implementação bem-sucedida das ações e para a manutenção da conformidade no longo prazo.

6.1. Continuidade do Trabalho

Os próximos passos para a implementação e acompanhamento das medidas de segurança e conformidade podem incluir as seguintes ações:

I. Execução do Plano de Ação: Iniciar a implementação das ações corretivas e de melhoria identificadas, com foco nas áreas críticas que precisam de ajustes, como a documentação dos processos, a implementação de controles de segurança mais robustos e o treinamento contínuo dos colaboradores.

II. Definição de Responsáveis e Cronograma: Atribuir responsáveis por cada ação dentro do plano e estabelecer um cronograma claro para a execução das medidas. Isso inclui a definição de metas intermediárias para garantir o progresso contínuo e avaliar a eficácia das ações.

III. Desenvolvimento e Atualização de Políticas e Procedimentos: Atualizar as políticas internas de segurança da informação, garantindo que estejam alinhadas com os requisitos das normas ISO 27001 e ISO 27002. Isso também inclui a criação de novos procedimentos, especialmente para áreas que ainda não estão suficientemente documentadas, como o gerenciamento de riscos de fornecedores e a inteligência contra ameaças.

IV. Monitoramento Contínuo e Avaliação de Resultados: Implementar um sistema de monitoramento contínuo para avaliar o progresso das ações e a eficácia dos controles de segurança. Isso pode incluir a realização de auditorias internas regulares, revisões periódicas dos processos e a avaliação contínua dos riscos.

V. Treinamento e Conscientização Contínuos: Desenvolver e realizar treinamentos regulares em segurança da informação para todos os colaboradores, com foco nas melhores práticas e na importância das políticas implementadas. Programas de conscientização também devem ser realizados para garantir que todos estejam alinhados com as políticas de segurança.

VI. Revisão e Melhoria Contínua: Com base nas auditorias e nos feedbacks recebidos, revisar periodicamente as políticas e os processos, ajustando-os conforme necessário. A melhoria contínua é essencial para garantir que a organização esteja sempre em conformidade com as normas ISO e alinhada às melhores práticas de segurança.

VII. Engajamento da Alta Direção: Garantir que a alta direção continue comprometida com o processo de conformidade, apoiando as iniciativas de segurança e garantindo que os recursos necessários estejam disponíveis para a implementação das ações. Isso inclui manter a alta direção informada sobre o progresso e os resultados das medidas implementadas.

VIII. Avaliação e Atualização daa Estrutura NIST: Como a empresa já utiliza a estrutura NIST, é importante avaliar periodicamente se a estrutura está sendo seguida de forma eficaz, ajustando as estratégias e as operações conforme necessário para manter a conformidade.

Esses passos permitirão garantir a continuidade das melhorias de segurança e a proteção constante dos ativos críticos da organização, além de assegurar que a empresa esteja preparada para responder a qualquer novo desafio ou ameaça que possa surgir.

6.2. Limitações do Estudo

As limitações do estudo podem ser apresentadas em diversos aspectos, que refletem desafios e restrições enfrentadas durante o processo de análise. Algumas possíveis limitações incluem:

I. Acesso Restrito a Informações Sensíveis: Devido à natureza da empresa, que atua no setor financeiro e possui capital aberto, o acesso a informações sensíveis foi restrito. Isso limitou a capacidade de explorar em detalhes alguns processos internos, o que pode ter afetado a profundidade da análise em determinadas áreas da segurança da informação.

II. Escopo Restrito ao Setor de Pagamentos: O estudo focou apenas nas operações de Pagamentos S.A., que são as mais consolidadas dentro da empresa. Embora essa abordagem tenha permitido uma análise mais precisa, ela não contemplou outras áreas da organização, o que pode ter gerado uma visão incompleta da segurança da informação em toda a empresa.

III. Disponibilidade de Dados: A coleta de dados foi limitada a informações disponíveis, como relatórios internos e entrevistas com alguns funcionários-chave. A falta de dados mais abrangentes ou de uma análise quantitativa mais profunda pode ter influenciado a robustez de algumas das conclusões.

IV. Tempo Limitado para Realização das Entrevistas: As entrevistas com os funcionários-chave tiveram uma duração média de 30 minutos. Esse tempo pode ter sido insuficiente para explorar com maior profundidade todas as questões e preocupações em relação à segurança da informação, além de limitar a quantidade de informações obtidas.

V. Percepção dos Participantes: O estudo se baseou nas percepções dos entrevistados em relação aos processos e práticas de segurança. Isso pode introduzir um viés subjetivo nas respostas, dependendo da experiência, do entendimento e da visão de cada participante sobre os controles de segurança e sua eficácia.

VI. Mudanças no Cenário de Cibersegurança: A segurança da informação é um campo dinâmico e sujeito a rápidas mudanças. O estudo foi realizado em um determinado ponto no tempo, e as conclusões podem não refletir as condições de segurança da informação da empresa ao longo do tempo, especialmente diante de novas ameaças cibernéticas ou mudanças tecnológicas.

VII. Subjetividade na Avaliação de Riscos: A matriz de risco qualitativa depende da interpretação subjetiva dos entrevistados e da equipe responsável pela avaliação. A atribuição de riscos em categorias qualitativas como "alto", "médio" e "baixo" pode variar dependendo da percepção de cada pessoa, o que pode introduzir viés nas análises e resultar em avaliações que não refletem com precisão a gravidade dos riscos. Como a matriz qualitativa utiliza classificações subjetivas, ela pode não permitir comparações fáceis entre diferentes riscos ou mesmo entre diferentes organizações. Isso limita a capacidade de aplicar padrões mais amplos ou fazer comparações.

Essas limitações devem ser levadas em consideração ao interpretar os resultados do estudo e ao implementar as recomendações, pois podem afetar a abrangência e a aplicabilidade dos achados.

7. REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO/IEC 27001:2022. **Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos**.

ABNT NBR ISO/IEC 27002:2022. **Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação**.

ABNT NBR ISO 31000:2018. **Gestão de riscos – Diretrizes**.

ACHMADI, Dedy; SURYANTO, Yohan; RAMLI, Kalamullah. On developing information security management system (isms) framework for iso 27001-based data center. In: **2018 International Workshop on Big Data and Information Security (IWBIS)**. IEEE, 2018. p. 149-157.

ALDYA, A. P.; SUTIKNO, S.; ROSMANSYAH, Y. Measuring effectiveness of control of information security management system based on SNI ISO/IEC 27004: 2013 standard. In: **IOP Conference Series: Materials Science and Engineering**. IOP Publishing, 2019. p. 012020.

ANANT, V.; DONCHAK, L.; KAPLAN, J.; SOLLER, H. **The consumer-data opportunity and the privacy imperative**. McKinsey & Company, 27 abr. 2020. Disponível em: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative. Acesso em: 11 set. 2024.

ASSI, Marcos. Gestão de riscos com controles internos. São Paulo: Saint Paul Editora, 2021.

BOEHMER, Wolfgang. Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001. In: **2008 Second International Conference on Emerging Security Information, Systems and Technologies**. IEEE, 2008. p. 224-231.

CHAUDHURI, Abhik; BOZKUS KAHYAOGLU, Sezer. Cybersecurity assurance in smart cities: A risk management perspective. **EDPACS**, v. 67, n. 4, p. 1-22, 2023.

CHECK POINT RESEARCH. **Check Point Research reports highest increase of global cyber attacks seen in last two years – a 30% increase in Q2 2024 global cyber attacks**. Disponível em: https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/. Acesso em: 15 out. 2024.

CISO ADVISOR. **Ataques crescem cerca de 70% no Brasil em um ano**. Disponível em: https://www.cisoadvisor.com.br/ataques-crescem-cerca-de-70-no-brasil-em-um-ano/#:~:text=O%20aumento%20global%20dos%20ataques,ao%20primeiro%20trimestre%20de%202024. Acesso em: 16 out. 2024.

CREADO, Yorrick; RAMTEKE, Vidyavati. Active cyber defence strategies and techniques for banks and financial institutions. **Journal of Financial Crime**, v. 27, n. 3, p. 771-780, 2020.

CULOT, Giovanna et al. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. **The TQM Journal**, v. 33, n. 7, p. 76-105, 2021.

DIDRAGA, Otniel et al. CHARACTERISTICS OF EFFECTIVE IT PROJECT RISK MANAGEMENT IN ROMANIAN IT COMPANIES. **Economic Computation & Economic Cybernetics Studies & Research**, v. 53, n. 4, 2019.

DISTERER, Georg. ISO/IEC 27000, 27001 and 27002 for information security management. **Journal of Information Security***,* v. 4, n. 2, 2013.

DUIJM, Nijs Jan. Recommendations on the use and design of risk matrices. **Safety science**, v. 76, p. 21-31, 2015.

ESTRATÉGIA CONCURSOS. **Segurança da informação: ISO 27002:2022. 2022**. Disponível em: https://www.estrategiaconcursos.com.br/blog/seguranca-informacao-iso-27002-2022/. Acesso em: 20 out. 2024.

GLOBO, O. **Incidentes cibernéticos em sistemas do governo dobram no primeiro semestre de 2024**. O Globo, 24 jul. 2024. Disponível em: https://oglobo.globo.com/politica/noticia/2024/07/24/incidentes-ciberneticos-em-sistemas-do-governo-dobram-no-primeiro-semestre-de-2024.ghtml. Acesso em: 17 out. 2024.

HASAN, Morshadul; HOQUE, Ariful; LE, Thi. Big data-driven banking operations: Opportunities, challenges, and data security perspectives. **FinTech**, v. 2, n. 3, p. 484-509, 2023.

HARUNA, Williams; AREMU, Toyin Ajiboro; MODUPE, Yetunde Ajao. Defending against cybersecurity threats to the payments and banking system. **arXiv preprint** arXiv:2212.12307, 2022.

HINTZBERGEN, Jule et al. **Fundamentos de segurança da informação: com base na ISO 27001 e na ISO 27002**. 1. ed. Rio de Janeiro: Brasport, 2018.

Humanperf. **5W1H glossary: definition, method and practical use**, 2023. Disponível em: https://www.humanperf.com/en/blog/nowiunderstand-glossary/articles/5W1H-method. Acesso em: 22 set. 2024.

ISO/IEC 27001:2022. **Information security, cybersecurity and privacy protection — Information security management systems — Requirements**. 3. ed. Geneva: ISO, 2022. Disponível em: https://www.iso.org/standard/27001. Acesso em: 26 ago. 2024.

ISO/IEC 27002:2022. **Information security, cybersecurity and privacy protection — Information security controls**. 3. ed. Geneva: ISO, 2022. Disponível em: https://www.iso.org/standard/75652.html. Acesso em: 26 ago. 2024.

ISO 31000:2018. **Gestão de riscos — Diretrizes**. Genebra: ISO, 2018. Disponível em: https://www.iso.org/standard/65694.html. Acesso em: 29 ago. 2024.

JAKÁBOVÁ, Martina; URDZIKOVÁ, Jana; MIRONOVOVÁ, Emília. Standardization of Information Security Management System: ISO/IEC 27001: 2005, ITIL®, CoBIT®. **International Journal of Recent Contributions from Engineering, Science & IT (iJES)**, v. 1, n. 2, p. 11-18, 2013.

JIA, Changjiang et al. 5W+ 1H pattern: A perspective of systematic mapping studies and a case study on cloud software testing. **Journal of Systems and Software**, v. 116, p. 206-219, 2016

JOHNSON, Robert; EASTTOM, Chuck. **Security policies and implementation issues**. Sudbury: Jones & Bartlett Learning, 2020.

KNEPPER, Hillary. Designing And Managing Programs: An Effectiveness-based Approach, by Peter M. Kettner, Robert M. Moroney, and Lawrence L. Martin: Thousand Oaks, CA: Sage Publications, 2008, 275 pages. 2009.

KETTNER, Peter M.; MORONEY, Robert M.; MARTIN, Lawrence L. **Designing and managing programs: An effectiveness-based approach**. Sage Publications, 2015.

KITSIOS, Fotis; CHATZIDIMITRIOU, Elpiniki; KAMARIOTOU, Maria. Developing a risk analysis strategy framework for impact assessment in information security management systems: A case study in it consulting industry. **Sustainability**, v. 14, n. 3, p. 1269, 2022.

LANDOLL, Douglas J. **Information security policies, procedures, and standards: a practitioner's reference**. Boca Raton: Auerbach Publications, 2017.

LAMARCA, Bryan Irvin. Cybersecurity risk assessment of the university of northern Philippines using PRISM approach. In: IOP Conference Series: Materials Science and Engineering. **IOP Publishing**, 2020. p. 012066.

LOWRY, Oliver H. et al. Protein measurement with the Folin phenol reagent. **J biol Chem**, v. 193, n. 1, p. 265-275, 1951.

MABROUKI, Charif; BENTALEB, Fatimazahra; MOUSRIJ, Ahmed. A decision support methodology for risk management within a port terminal. **Safety Science**, v. 63, p. 124-132, 2014.

MAKRIDIS, Christos A. Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018. **Journal of Cybersecurity**, v. 7, n. 1, p. tyab021, 2021.

MCKINSEY & COMPANY. **What is cybersecurity**. Disponível em: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-cybersecurity. Acesso em: 12 nov. 2024.

Medium, **How to use the 5W1H rule?**, 2023. Disponível em: https://medium.com/deepak-chawla/5w1h-rule-2c2d2ed1cddd?source=post_internal_links----------2----------. Acesso em: 22 set. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Framework for Improving Critical Infrastructure Cybersecurity**. April 16, 2018. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Acesso em: 26 ago. 2024.

NIST. **Cybersecurity**. Disponível em: https://www.nist.gov/cybersecurity. Acesso em: 26 ago. 2024.

OKPAMEN, Peter. Security requirements, analysis and policy formulation for educational institutions. **Journal of Educational and Social Research**, v. 3, n. 5, p. 93-102, 2013.

PELTIER, Thomas R. **Information security policies, procedures, and standards: guidelines for effective information security management**. Boca Raton: CRC Press, 2016.

PIMCHANGTHONG, Daranee; BOONJING, Veera. Effects of risk management practice on the success of IT project. **Procedia Engineering**, v. 182, p. 579-586, 2017.

PROJECT MANAGEMENT INSTITUTE (PMI). **A Guide to the Project Management Body of Knowledge (Guia PMBOK®)**. 7.ed. [S.l.]: Project Management Institute Inc., 2021

RAMPINI, Gabriel Henrique Silva; TAKIA, Harmi; BERSSANETI, Fernando Tobal. Critical success factors of risk management with the advent of ISO 31000 2018-Descriptive and content analyzes. **Procedia Manufacturing**, v. 39, p. 894-903, 2019.

RAMPINI, Gabriel Henrique Silva; BERSSANETI, Fernando Tobal. Impact of critical success factors and risk management on organizational results. **Brazilian Journal of Operations & Production Management**, v. 21, n. 1, p. 1412-1412, 2024.

RAMIREZ, Robert; CHOUCRI, Nazli. Improving interdisciplinary communication with standardized cyber security terminology: a literature review. **IEEE Access**, v. 4, p. 2216-2243, 2016.

ROY, Prameet P. A high-level comparison between the nist cyber security framework and the iso 27001 information security standard. In: 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA). **IEEE, 2020**. p. 1-3.

SAEED, Saqib et al. Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. **Sensors**, v. 23, n. 15, p. 6666, 2023.

SCHILIRO, Francesco. Towards a Contemporary Definition of Cybersecurity. **arXiv preprint** arXiv:2302.02274, 2023.

SHEN, Yuying; BUCHANAN TURNER, Carlene; TURNER, Claude. Cybersecurity Training in Organization as Human Capital Investment: **A Qualitative Grounded Theory Analysis. International Journal of Business and Management**, v. 18, n. 4, 2023.

SRINIVASAN, K.; RAJARAJESWARI, S. Financial technology in Indian finance market. **Available at SSRN 3845245**, 2021.

SU, Xiao. The application of “5W1H” in industrial design. **Advanced materials research**, v. 1028, p. 346-349, 2014.

UDDIN, Md Hamid; ALI, Md Hakim; HASSAN, Mohammad Kabir. Cybersecurity hazards and financial system vulnerability: a synthesis of literature. **Risk Management**, v. 22, n. 4, p. 239-309, 2020.

APÊNDICE A

Contexto

O objetivo desta entrevista é avaliar a eficácia dos controles de segurança da informação implementados na empresa, de acordo com as normas ISO/IEC 27001 e ISO/IEC 27002. Essas normas são essenciais para garantir a segurança, confidencialidade, integridade e disponibilidade das informações. Sabendo que a organização possui diretrizes associadas a essas normas, esta entrevista visa entender como esses controles estão sendo aplicados, identificar eventuais problemas e destacar aspectos positivos. O material coletado será utilizado para construir um diagnóstico que direcione a empresa no processo de gestão de segurança da informação em conformidade com as normas ISO/IEC 27001 e ISO/IEC 27002.

OBS:

1) Todas as perguntas permitem justificativas adicionais, a critério do entrevistado.
2) Algumas perguntas podem ser ajustadas conforme o cenário apresentado.

E1 - Diretor de Engenharia

(E1.1) Como você avalia a eficácia dos controles de segurança da informação atualmente implementados na empresa?

(E1.2) Quais são os principais desafios que você enfrenta na gestão de riscos de segurança da informação?

(E1.3) Existem áreas específicas onde você vê necessidade de melhorias significativas nos controles de segurança?

E2 - Gerente de Riscos de Tecnologia da Informação

(E2.1) Quais são as medidas de segurança implementadas para proteger a rede e os sistemas da empresa?

(E2.2) Como é realizada a gestão de mudanças nos sistemas de TI? Existe um processo formalizado?

(E2.3) Quais são os principais tipos de ataques cibernéticos que a empresa enfrenta atualmente?

(E2.4) Como a equipe de TI é treinada para lidar com incidentes de segurança da informação?

(E2.5) Você acredita que os recursos atuais (tecnológicos e humanos) são suficientes para garantir a segurança da informação?

(E2.6) Como a empresa lida com a gestão de riscos de fornecedores em termos de segurança da informação?

E3 - Gerente de Segurança da Informação

(E3.1) Quais são as ferramentas e metodologias utilizadas para avaliar e mitigar vulnerabilidades técnicas?

(E3.2) Como você descreve o processo de gestão de riscos dentro da empresa?

(E3.3) Quais são as principais políticas de segurança da informação com as quais você trabalha diariamente?

(E3.4) Como são gerenciados os riscos de segurança da informação relacionados a fornecedores?

(E3.5) Quais são os principais desafios que você enfrenta na gestão da segurança da informação?

E4 - Gerente de Engenharia

(E4.1) Como é realizado o monitoramento e registro de atividades para detectar atividades suspeitas?

(E4.2) Quais são os controles de acesso implementados para garantir que apenas usuários autorizados acessem informações sensíveis?

(E4.3) Como são realizados os treinamentos e a conscientização sobre segurança da informação para os funcionários?

(E4.4) Você percebe alguma lacuna nos controles de segurança atuais que poderiam ser melhorados?

ANEXO A

Quadro A.1: Processos da NIST

Processos
ID.RM-3: A determinação da tolerância ao risco da organização é informada pelo seu papel nas infra-estruturas críticas e na análise de risco específica do sector
ID.BE-4: São estabelecidas dependências e funções críticas para a prestação de serviços críticos
ID.BE-3: As prioridades para a missão, objectivos e actividades da organização são estabelecidas e comunicadas
ID.AM-1: Os dispositivos e sistemas físicos da organização são inventariados
ID.AM-3: A comunicação organizacional e os fluxos de dados são mapeados
ID.BE-5: Os requisitos de resiliência para apoiar a prestação de serviços críticos são estabelecidos para todos os estados operacionais (por exemplo, sob coação/ataque, durante a recuperação, operações normais)
ID.RA-5: Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar o risco
ID.SC-4: Os fornecedores e parceiros de terceiros são avaliados regularmente para confirmar que estão a cumprir as suas obrigações contratuais. São efectuadas análises de auditorias, resumos de resultados de testes ou outras avaliações equivalentes de fornecedores
ID.RM-2: A tolerância ao risco organizacional é determinada e claramente expressa
ID.SC-3: Os fornecedores e parceiros de terceiros são obrigados por contrato a implementar medidas apropriadas concebidas para cumprir os objectivos do programa de Segurança da Informação ou do Plano de Gestão do Risco da Cadeia de Abastecimento Cibernético
ID.AM-4: Os sistemas de informação externos são catalogados
ID.RA-2: A informação sobre ciberameaças é recebida de fóruns e fontes de partilha de informação
ID.SC-5: O planeamento e os testes de resposta e recuperação são realizados com fornecedores e prestadores de serviços terceiros
ID.RA-4: São identificados os potenciais impactos e probabilidades de negócio
ID.AM-6: São estabelecidas funções e responsabilidades de cibersegurança para toda a força de trabalho e partes interessadas terceiras (por exemplo, fornecedores, clientes, parceiros)
ID.RA-6: As respostas aos riscos são identificadas e priorizadas
ID.SC-2: Identificar, priorizar e avaliar fornecedores e parceiros terceiros de sistemas de informação, componentes e serviços usando um processo de avaliação de risco da cadeia de fornecimento cibernético
ID.RM-1: Os processos de gestão de risco são estabelecidos, geridos e aceites pelas partes interessadas da organização
ID.AM-2: As plataformas e aplicações de *software* da organização são inventariadas
ID.GV-1: A política de segurança da informação da organização é estabelecida
ID.GV-3: Os requisitos legais e regulamentares relativos à cibersegurança, incluindo as obrigações de privacidade e liberdades civis, são compreendidos e geridos
ID.RA-3: As ameaças, tanto internas como externas, são identificadas e documentadas
ID.AM-5: Os recursos (por exemplo, *hardware*, dispositivos, dados, tempo e *software*) são priorizados com base na sua classificação, criticidade e valor comercial
ID.GV-4: Os processos de governação e gestão de risco abordam os riscos de cibersegurança
ID.BE-2: A posição da organização na infraestrutura crítica e no seu sector de atividade é identificada e

comunicada
ID.GV-2: As funções e responsabilidades da segurança da informação são coordenadas e alinhadas com as funções internas e os parceiros externos
ID.BE-1: O papel da organização na cadeia de abastecimento é identificado e comunicado
ID.SC-1: Os processos de gestão do risco da cadeia de abastecimento cibernético são identificados, estabelecidos, avaliados, geridos e aceites pelas partes interessadas da organização
ID.RA-1: As vulnerabilidades dos activos são identificadas e documentadas
PR.MA-1: A manutenção e a reparação dos activos da organização são realizadas e registadas atempadamente, com ferramentas aprovadas e controladas
PR.IP-12: Um plano de gestão de vulnerabilidades é desenvolvido e implementado
PR.IP-11: A cibersegurança está incluída nas práticas de recursos humanos (por exemplo, desprovisionamento, seleção de pessoal)
PR.IP-9: Planos de resposta (Resposta a Incidentes e Continuidade do Negócio) e planos de recuperação (Recuperação de Incidentes e Recuperação de Desastres) estão em vigor e são geridos
PR.IP-8: A eficácia das tecnologias de proteção é partilhada com as partes apropriadas
PR.IP-7: Os processos de proteção são continuamente melhorados
PR.IP-5: A política e os regulamentos relativos ao ambiente operacional físico dos ativos da organização são cumpridos
PR.IP-3: Os processos de controle de alterações de configuração estão em vigor
PR.IP-4: As cópias de segurança da informação são efectuadas, mantidas e testadas periodicamente
PR.DS-4: Capacidade adequada para garantir a disponibilidade é mantida
PR.AC-2: O acesso físico aos activos é gerido e protegido
PR.DS-8: Mecanismos de verificação de integridade são usados para verificar a integridade do *hardware*
PR.DS-6: Mecanismos de verificação da integridade são usados para verificar a integridade do *software*, do firmware e da informação
PR.IP-2: Um ciclo de vida de desenvolvimento de sistema para gerenciar sistemas é implementado
PR.DS-5: Proteção contra vazamento de dados são implementadas
PR.IP-1: É criada e mantida uma configuração de base das tecnologias de informação/sistemas de controle industrial, incorporando princípios de segurança adequados (por exemplo, o conceito de funcionalidade mínima)
PR.DS-3: Os activos são formalmente geridos durante a sua remoção, transferência e eliminação
PR.DS-2: Os dados em trânsito são protegidos
PR.AC-5: A integridade da rede é protegida, incorporando a segregação da rede quando apropriado
PR.AT-4: Os executivos de topo compreendem as funções e responsabilidades
PR.AT-5: O pessoal de segurança física e da informação compreende as funções e responsabilidades
PR.IP-6: Os dados são destruídos de acordo com a política
PR.AT-3: As partes interessadas de terceiros (por exemplo, fornecedores, clientes, parceiros) compreendem as funções e responsabilidades
PR.AT-2: Os utilizadores privilegiados compreendem as funções e responsabilidades
PR.IP-10: Os planos de resposta e recuperação são testados

PR.DS-7: O(s) ambiente(s) de desenvolvimento e teste são separados do ambiente de produção
PR.DS-1: Os dados em repouso são protegidos
PR.AT-1: Todos os utilizadores são informados e formados
PR.AC-7: Os utilizadores, os dispositivos e outros activos são autenticados (por exemplo, fator único, multi-fator) e proporcionais ao risco da transação (por exemplo, riscos de segurança e privacidade dos indivíduos e outros riscos organizacionais)
PR.MA-2: A manutenção remota dos activos da organização é aprovada, registrada e executada de forma a impedir o acesso não autorizado
PR.AC-4: As permissões e autorizações de acesso são geridas, incorporando os princípios do menor privilégio e da separação de funções
PR.AC-6: A identidade do utilizador é verificada durante a emissão de uma credencial e é sistematicamente comprovada ao longo da sua vida útil.
PR.AC-3: O acesso remoto é gerenciado
PR.PT-5: Os sistemas operam em estados funcionais pré-definidos para alcançar a disponibilidade (por exemplo, sob coação, sob ataque, durante a recuperação, operações normais)
PR.PT-4: As redes de comunicação e controle são protegidas
PR.PT-3: O princípio da menor funcionalidade é incorporado através da configuração de sistemas para fornecer apenas as capacidades essenciais
PR.PT-2: Os meios de comunicação amovíveis são protegidos e a sua utilização é restringida de acordo com a política
PR.PT-1: Os registos de auditoria/log são determinados, documentados, implementados e revistos de acordo com a política
PR.AC-1: As identidades e credenciais são emitidas, geridas, verificadas, revogadas e auditadas para dispositivos, utilizadores e processos autorizados
DE.AE-2: Os eventos detectados são analisados para compreender os alvos e métodos de ataque
DE.AE-1: É estabelecida e gerida uma linha de base das operações de rede e dos fluxos de dados esperados para utilizadores e sistemas
DE.DP-3: Os processos de detecção são testados
DE.DP-4: A informação sobre a deteção de eventos é comunicada às partes apropriadas
DE.CM-8: São efectuadas análises de vulnerabilidades
DE.DP-2: As actividades de detecção cumprem todos os requisitos aplicáveis
DE.DP-1: As funções e responsabilidades pela deteção estão bem definidas para garantir a responsabilização
DE.CM-7: É efectuada a monitorização de pessoal, ligações, dispositivos e *software* não autorizados
DE.CM-6: A atividade dos fornecedores de serviços externos é monitorada para detectar potenciais eventos de cibersegurança
DE.CM-5: O código móvel não autorizado é detectado
DE.CM-4: Detecção de código malicioso
DE.CM-3: A atividade do pessoal é monitorada para detectar potenciais eventos de cibersegurança
DE.DP-5: Os processos de detecção são continuamente melhorados
DE.CM-2: O ambiente físico é monitorizado para detetar potenciais eventos de cibersegurança
DE.CM-1: A rede é monitorada para detectar potenciais eventos de cibersegurança

DE.AE-5: São estabelecidos limiares de alerta de incidentes
DE.AE-4: O impacto dos eventos é determinado
DE.AE-3: Os dados dos eventos são recolhidos e correlacionados a partir de múltiplas fontes e sensores
RS.IM-2: As estratégias de resposta são actualizadas
RS.MI-3: As vulnerabilidades recentemente identificadas são atenuadas ou documentadas como riscos aceites
RS.MI-2: Os incidentes são mitigados
RS.MI-1: Os incidentes são contidos
RS.AN-4: Os incidentes são categorizados de acordo com os planos de resposta
RS.AN-3: A investigação forense é efectuada
RS.AN-2: O impacto do incidente é compreendido
RS.AN-1: As notificações dos sistemas de deteção são investigadas
RS.CO-5: A partilha voluntária de informações ocorre com as partes interessadas externas para alcançar um conhecimento mais amplo da situação da cibersegurança
RS.CO-4: A coordenação com as partes interessadas é efectuada de acordo com os planos de resposta
RS.CO-3: A informação é partilhada de acordo com os planos de resposta
RS.AN-5: Os processos são estabelecidos para receber, analisar e responder às vulnerabilidades divulgadas à organização a partir de fontes internas e externas (por exemplo, testes internos, boletins de segurança ou investigadores de segurança)
RS.CO-2: Os incidentes são relatados de acordo com os critérios estabelecidos
RS.CO-1: O pessoal conhece as suas funções e a ordem de operações quando é necessária uma resposta
RS.IM-1: Os planos de resposta incorporam as lições aprendidas
RS.RP-1: O plano de resposta é executado durante ou após um incidente
RC.CO-3: As actividades de recuperação são comunicadas às partes interessadas internas e às equipes executivas e de gestão
RC.CO-2: A reputação após um evento é reparada
RC.CO-1: As relações públicas são geridas
RC.IM-2: As estratégias de recuperação são actualizadas
RC.IM-1: Os planos de recuperação incorporam as lições aprendidas
RC.RP-1: O plano de recuperação é executado durante ou após um incidente de cibersegurança

Fonte: NIST