ISSN 1678-0817 Qualis B2

ANÁLISE DO PROCESSO DE IMPLEMENTAÇÃO DE UM SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO COM BASE NA ISO/IEC 27001

Ciências Exatas e da Terra, Volume 29 - Edição 142/JAN 2025 / 19/01/2025

REGISTRO DOI: 10.69849/revistaft/pa10202501192208

Carlos Henrique Leão Chagas[1]

Andrew Hemerson Galeno Rodrigues[2]

Resumo

O tema desta pesquisa é a implementação de um Sistema de Gestão de Segurança da Informação (SGSI) com base na norma ISO/IEC 27001 em uma organização da área de tecnologia da informação. O objetivo principal foi analisar o processo de implantação do SGSI, abordando as etapas do ciclo PDCA (Planejar, Fazer, Veri car, Agir) e os desa os enfrentados pela organização. A metodologia adotada foi qualitativa e exploratória, utilizando estudo de caso, observação participante e análise documental para identi car ativos, avaliar riscos e implementar controles de segurança. Os principais resultados evidenciaram melhorias signi cativas na governança da segurança da informação, com aumento da resiliência frente a ameaças cibernéticas, fortalecimento da con ança de clientes e otimização de processos internos. A matriz de riscos e o plano de tratamento de risco destacaram- se como ferramentas e cazes na priorização de ações corretivas e alocação de recursos. Conclui-se que, embora a certi cação formal da ISO/IEC 27001 ainda não tenha sido obtida, a implementação do SGSI resultou em avanços notáveis na

proteção dos ativos informacionais, contribuindo para a conformidade regulatória e a cultura organizacional voltada à segurança. O estudo oferece insights práticos para organizações que buscam aprimorar suas estratégias de gestão da segurança da informação.

Palavras-chave: Segurança da informação. ISO 27001. SGSI. Tecnologia da informação.

Abstract

The theme of this research is the implementation of an Information Security Management System (ISMS) based on the ISO/IEC 27001 standard in an information technology organization. The main objective was to analyze the ISMS implementation process, addressing the stages of the PDCA cycle (Plan, Do, Check, Act) and the challenges faced by the organization. The methodology adopted was qualitative and exploratory, using case study, participant observation and document analysis to identify assets, assess risks and implement security controls. The main results showed signi cant improvements in information security governance, with increased resilience against cyber threats, strengthening customer con dence and optimizing internal processes. The risk matrix and the risk treatment plan stood out as effective tools in prioritizing corrective actions and allocating resources. It is concluded that, although formal ISO/IEC 27001 certi cation has not yet been obtained, the implementation of the ISMS has resulted in notable advances in the protection of information assets, contributing to regulatory compliance and a security-oriented organizational culture. The study offers practical insights for organizations seeking to improve their information security management strategies.

Keywords: Information security. ISO 27001. ISMS. Information technology.

1. Introdução

A crescente dependência das organizações em sistemas informatizados e a intensi cação das trocas de dados no ambiente virtual tornam a segurança da informação um fator primordial para garantir a con abilidade dos processos corporativos e a proteção dos ativos organizacionais. Nesse contexto, a implementação de elementos de segurança, como políticas de acesso, criptogra a, backups e

monitoramento contínuo, visa atenuar vulnerabilidades que podem comprometer a integridade e a disponibilidade das informações (STALLINGS, 2016). Além disso, a capacidade de assegurar a con dencialidade dos dados é um diferencial competitivo que in ui diretamente na credibilidade institucional, sendo esta uma preocupação constante em diversos setores, como o nanceiro, o governamental e o de saúde (LAUDON; LAUDON, 2018). A insu ciência desses elementos pode resultar em incidentes graves de violação de dados, ocasionando prejuízos nanceiros e danos à reputação da organização. Por conseguinte, a adoção de uma política robusta de segurança da informação proporciona diretrizes mais claras e objetivas, estabelecendo um arcabouço sólido para a mitigação de ameaças internas e externas (WHITMAN; MATTORD 2017).

A norma ISO/IEC 27001 se destaca como um referencial internacionalmente reconhecido na implementação das melhores práticas de segurança da informação (ISO/IEC, 2013). Seu escopo abrange a de nição de requisitos, processos e controles de segurança, com o objetivo de estabelecer e manter um Sistema de Gestão de Segurança da Informação (SGSI) capaz de se adaptar às necessidades especí cas de cada organização (ABNT, 2013).

A norma propõe uma estrutura sistemática para a identi cação, avaliação e tratamento de riscos, englobando desde a formulação de políticas de segurança até mecanismos de auditoria e melhoria contínua. Sob essa perspectiva, a ISO/IEC 27001 exige comprometimento estratégico da alta direção, de modo que as práticas de segurança sejam efetivamente incorporadas à cultura organizacional (REZENDE; ABREU, 2018). Dessa forma, a adoção desse padrão confere não apenas maior proteção, mas também assegura conformidade com legislações e regulamentações em diversos segmentos de mercado.

O objetivo principal da pesquisa é investigar o processo de implementação de um Sistema de Gestão da Segurança da Informação (SGSI) em conformidade com a norma ISO/IEC 27001, em uma empresa da área de tecnologia da informação. A metodologia aplicada no estudo seguiu um enfoque qualitativo e exploratório, utilizando o método de estudo de caso para detalhar o processo de implementação de um Sistema de Gestão da Segurança da Informação (SGSI) conforme a norma ISO/IEC 27001. Foram realizadas análises detalhadas dos processos e práticas da organização, com base no ciclo PDCA (Planejar,

Fazer, Veri car, Agir), abrangendo a identi cação de ativos, avaliação de riscos, tratamento de vulnerabilidades e a implementação de controles de segurança.

2. Referencial Teórico

2.1 ISO 27001

A ISO 27001 é amplamente reconhecida como um padrão internacional para sistemas de gestão da segurança da informação (ISMS). Ela estabelece uma abordagem sistemática para proteger a con dencialidade, integridade e disponibilidade das informações, essenciais para a operação de qualquer organização moderna (DISTERER, 2013). O cumprimento de seus requisitos implica não apenas na mitigação de riscos cibernéticos, mas também na construção de uma cultura organizacional voltada à segurança e conformidade regulatória.

A implementação da ISO 27001 envolve etapas críticas, incluindo a identi cação de ativos informacionais, análise de riscos e desenvolvimento de controles apropriados. O método PDCA (Plan-DoCheck-Act) é frequentemente adotado para garantir a melhoria contínua dos processos de segurança (GUO et al., 2021). Este ciclo garante que a gestão de riscos e os controles sejam revisados e aprimorados regularmente, fortalecendo a postura de segurança da organização.

Empresas que adotam a ISO 27001 bene ciam-se de maior resiliência contra incidentes de segurança, além de ganhos em reputação e

competitividade. No setor bancário, por exemplo, a certi cação tem sido crucial para atender a requisitos de conformidade e aumentar a con ança dos clientes (EWUGA et al., 2024). A capacidade de demonstrar conformidade com padrões internacionais também facilita a obtenção de novos negócios em setores regulados.

Um dos principais desa os enfrentados na implementação do ISMS baseado na ISO 27001 é o alinhamento entre os requisitos técnicos e as exigências organizacionais. Segundo Sharma e Dash (2012), mesmo empresas certi cadas podem apresentar lacunas em seus

sistemas, indicando a necessidade de uma abordagem mais integrada e focada em resultados práticos.

A ISO 27001 também desempenha um papel importante na promoção da gestão de riscos de forma abrangente. Ao integrar controles de segurança à governança corporativa, as empresas podem alinhar melhor suas práticas de segurança com os objetivos estratégicos, aumentando a e ciência operacional (UKIDVE; TADVALKAR, 2016). Esta integração ajuda a mitigar riscos nanceiros decorrentes de falhas de segurança, conforme evidenciado por análises empíricas de desempenho empresarial póscerti cação.

A revisão contínua do padrão ISO 27001, como a atualização de 2022, re ete a evolução das ameaças e das melhores práticas em segurança da informação. Vakhula et al. (2024) destacam a importância do controle de con guração (A.8.9), que reforça a necessidade de práticas robustas de segurança desde o desenvolvimento de software até a operação de sistemas.

Além de suas implicações operacionais, a certi cação ISO 27001 oferece benefícios signi cativos para a conformidade regulatória. Em muitos países, ela é utilizada como referência em políticas de segurança da informação, contribuindo para uma abordagem padronizada e con ável na proteção de dados (PUTRA et al., 2021). A ISO 27001 contribui não apenas para a proteção de ativos digitais, mas também para o desenvolvimento de parcerias estratégicas e con ança entre stakeholders. Ao demonstrar comprometimento com padrões internacionais de segurança, as empresas aumentam sua atratividade no mercado global e reduzem penalidades regulatórias em caso de incidentes (MILITARU, 2009).

2.2 Segurança da Informação

A segurança da informação é um campo essencial no ambiente corporativo e acadêmico, com o objetivo de proteger dados e sistemas contra ameaças internas e externas. De acordo com Stallings (2020), ela envolve a proteção da con dencialidade, integridade e disponibilidade da informação, considerando não apenas a proteção de dados digitais, mas também de informações em formato físico e verbal. Esses três pilares são amplamente reconhecidos como a base da segurança da informação.

O conceito de con dencialidade visa garantir que apenas pessoas autorizadas possam acessar as informações sensíveis. Segundo Tipton e Krause (2012), o controle de acesso é um dos principais mecanismos utilizados para assegurar a con dencialidade, que envolve autenticação, autorização e registro de ações dos usuários. Dessa forma, as organizações podem evitar a exposição indevida de dados.

A integridade refere-se à precisão e completude da informação. Conforme Ross et al. (2018), mecanismos como algoritmos de hash e assinaturas digitais são utilizados para veri car se a informação foi alterada de

maneira indevida durante a transmissão ou armazenamento. Isso assegura que os dados mantidos ou transmitidos permaneçam inalterados desde a sua criação.

A disponibilidade, por sua vez, garante que a informação esteja acessível sempre que necessária. Whitman e Mattord (2019) destacam que medidas como a implementação de backups regulares, redundância de sistemas e proteção contra ataques de negação de serviço (DDoS) são fundamentais para assegurar a continuidade do negócio e a disponibilidade de recursos.

Um dos principais desa os em segurança da informação é o gerenciamento de riscos. Segundo Peltier (2016), o processo de gerenciamento de riscos inclui a identi cação, análise e mitigacão de ameaças potenciais aos ativos de informação. A gestão e caz de riscos permite que as organizações minimizem perdas e se preparem para incidentes futuros.

A política de segurança da informação é um documento essencial para de nir regras e procedimentos. De acordo com Doherty e Fulford (2013), essa política deve ser desenvolvida com base nas necessidades especí cas de cada organização e revisada periodicamente. Uma política bem de nida ajuda a alinhar as ações de segurança com os objetivos de negócio.

Outro aspecto importante é a conscientização dos usuários. Gordon e Loeb (2015) enfatizam que a segurança da informação não depende apenas de tecnologia, mas

também do comportamento humano. Campanhas de educação e treinamentos regulares são e cazes para reduzir erros humanos e fraudes internas.

A criptogra a desempenha um papel fundamental na proteção de dados. De acordo com Schneier (2015), a criptogra a garante que mesmo que os dados sejam interceptados, eles não possam ser lidos sem a chave de decriptação apropriada. Isso se aplica tanto a dados em trânsito quanto a dados armazenados.

O monitoramento e a auditoria são essenciais para identi car e responder a incidentes de segurança. Segundo Northcutt (2014), o uso de ferramentas de monitoramento continuo permite que as organizações detectem anomalias e ameacem proativamente. Além disso, auditorias regulares ajudam a garantir a conformidade com normas e regulações.

A conformidade com normas e padrões internacionais é um requisito crescente. Segundo Calder e Watkins (2021), a adoção de padrões como ISO 27001 e NIST Cybersecurity Framework ajuda as organizações a estabelecer e manter um sistema de gestão de segurança e caz. A certi cação nesses padrões também aumenta a credibilidade perante clientes e parceiros.

2.2.1 Sistema de Gestão da Segurança da Informação

O Sistema de Gestão de Segurança da Informação (SGSI) pode ser de nido como um conjunto de políticas, processos e controles que uma organização implementa para proteger seus ativos de informação contra ameaças, garantindo a con dencialidade, integridade e disponibilidade das informações (Franco, 2014). Este sistema visa estabelecer uma abordagem sistemática para identi car riscos e aplicar medidas e cazes para mitigá-los, assegurando a continuidade das operações.

A implantação do SGSI depende de uma estratégia abrangente, que inclui o desenvolvimento de políticas de segurança e a de nição de procedimentos claros. Essa abordagem permite que as organizações estejam melhor preparadas para lidar com incidentes de segurança e minimizar os danos decorrentes de violações (Casaca e Correia, 2013). Além disso, a de nição de responsabilidades é crucial para garantir a e cácia das medidas implementadas.

De acordo com Marciano e Lima-Marques (2006), a segurança da informação não deve ser tratada apenas como uma questão tecnológica, mas como um equilíbrio entre aspectos humanos e técnicos. A interação dos colaboradores com os sistemas de informação é um fator determinante para o sucesso de um SGSI, exigindo treinamento e conscientização constantes.

Uma etapa fundamental na gestão de segurança da informação é a análise de riscos. Conforme Gualberto e Deus (2013), esse processo envolve a identi cação de vulnerabilidades e ameaças, bem como a avaliação de possíveis impactos. A implementação de controles deve ser orientada por essa análise, garantindo que os recursos sejam alocados de forma e ciente.

A ISO/IEC 27001 é a principal norma internacional que de ne os requisitos para um SGSI e caz. Segundo Silva (2016), essa norma oferece uma estrutura para o desenvolvimento de políticas e procedimentos que assegurem a proteção da informação e a conformidade com regulamentações legais e contratuais.

Além das questões técnicas, a gestão da segurança da informação requer o desenvolvimento de uma cultura organizacional que valorize a proteção dos dados. Santos et al. (2011) destacam que, para isso, é necessário um esforço contínuo na criação de ambientes que promovam a integridade e a responsabilidade dos funcionários no uso das informações.

A auditoria do SGSI é uma prática recomendada para garantir a conformidade e a e cácia do sistema. Segundo Vieira (2017), as auditorias internas e externas devem ser realizadas periodicamente para avaliar a adequação das medidas de segurança adotadas e identi car oportunidades de melhoria.

Outro conceito essencial no SGSI é a gestão de incidentes, que envolve a identi cação e o tratamento de eventos que possam comprometer a segurança da informação. Conforme Oliveira e Felipe (2013), a resposta

e caz a incidentes é vital para reduzir o tempo de inatividade e o impacto sobre os negócios.

A integração de tecnologias avançadas, como criptogra a e sistemas de autenticação multifatorial, é uma tendência crescente na gestão de segurança da informação. Pereira et al. (2011) ressaltam que essas tecnologias oferecem níveis adicionais de proteção, especialmente em ambientes que lidam com informações sensíveis.

A gestão da continuidade de negócios é um componente essencial de um SGSI. De acordo com Moraes et al. (2017), essa prática garante que a organização possa continuar operando mesmo diante de eventos adversos, minimizando prejuízos e mantendo a con ança dos stakeholders.

3. Metodologia

A metodologia adotada na presente pesquisa foi baseada em uma abordagem qualitativa e exploratória, com ênfase no estudo de caso de uma organização da área de tecnologia da informação. O principal objetivo foi analisar detalhadamente o processo de implementação de um Sistema de Gestão de Segurança da Informação (SGSI) em conformidade com a norma ISO/IEC 27001. A pesquisa seguiu uma abordagem estruturada, envolvendo etapas sistemáticas para coleta, análise e tratamento dos dados obtidos.

Este estudo caracteriza-se como qualitativo, por buscar compreender o fenômeno em profundidade, e exploratório, por investigar um tema complexo e com múltiplas variáveis envolvidas. A escolha pelo estudo de caso justi ca-se pela necessidade de detalhar o processo de implementação da norma em uma organização especí ca, permitindo compreender como as práticas de segurança foram adotadas e quais foram os principais desa os enfrentados durante o processo. A coleta de dados foi realizada por meio de observação participante, análise documental com os principais envolvidos no processo de implementação do SGSI. A observação participante permitiu acompanhar as etapas do projeto e registrar as práticas e procedimentos adotados. A análise documental envolveu o exame de relatórios internos, políticas de segurança, registros de auditorias e documentação técnica relacionada ao SGSI.

A pesquisa foi desenvolvida em cinco etapas principais:

. Planejamento: De nição do escopo da pesquisa, objetivos especí cos e metodologia a ser empregada. Nesta fase, também foi realizado o levantamento bibliográ co sobre a ISO/IEC 27001 e suas melhores práticas.

. Coleta de Dados: Compreendeu a aplicação das técnicas de coleta descritas anteriormente. As informações obtidas foram organizadas e categorizadas de acordo com as etapas do ciclo PDCA (Planejar, Fazer, Veri car, Agir) da norma ISO/IEC 27001.

. Análise de Dados: Os dados coletados foram analisados qualitativamente, com base nos princípios estabelecidos pela norma ISO/IEC 27001. A análise foi orientada para identi car os principais desa os, soluções implementadas e benefícios obtidos com a adoção do SGSI.

. Validação: Os resultados preliminares foram apresentados à equipe da organização, visando validar as informações coletadas e as interpretações realizadas. Sugestões e complementações foram incorporadas ao estudo.

. Elaboração do Relatório Final: Com a conclusão da análise, foi elaborado o relatório nal contendo a descrição detalhada do processo de implementação, os resultados obtidos e as conclusões da pesquisa.

A análise dos dados foi conduzida de forma indutiva, buscando-se identi car padrões e tendências emergentes a partir das informações coletadas. Foram utilizadas técnicas de análise de conteúdo para categorizar e interpretar os dados qualitativos, com ênfase nos seguintes aspectos:

- Identi cação de Ativos: Mapeamento dos ativos de informação da organização, incluindo sistemas, dados, infraestrutura e recursos humanos.
- Avaliação de Riscos: Análise das vulnerabilidades e ameaças associadas a cada ativo, com base nos critérios de probabilidade e impacto.
- Tratamento de Riscos: Descrição das medidas de controle implementadas para mitigar os riscos identi cados, incluindo controles técnicos, administrativos e operacionais.
- Monitoramento e Melhoria Contínua: Avaliação das práticas de monitoramento adotadas pela organização e identi cação de oportunidades de melhoria no SGSI.

4. Resultados e Discussões

4.1 Descrição da Empresa

Será apresentado e demonstrado um estudo de caso sobre uma organização que atua na área da tecnologia da informação e assim será detalhado o processo de implementação da ISO 27001 para garantia da implementação de um SGSI.

Para garantir a con abilidade dos dados disponíveis e apresentados da empresa no estudo de caso, o seu nome não será citado, pois todos os dados e informações disponibilizados tiveram essa condição, pois diversas especi cações e condições con denciais podem estar expostas nos resultados apresentados e assim podem fragilizar a imagem e percepções de mercado associadas a organização, dessa forma, para garantir a integridade e imagem da empresa seu nome não foi apresentado.

A empresa analisada atua na área de TI e possui pro ssionais que possuem profundo conhecimento do setor em uma ampla gama de organizações e setores verticais. A organização entende os desa os da implementação de novos sistemas de tecnologia da informação em um negócio e trabalha em estreita colaboração com os especialistas em TI e negócios de seus clientes para ajudá-los a identi car oportunidades e objetivos. Dessa forma, ela então se associa a eles para fornecer serviços completos do ciclo de vida do projeto, orquestrando efetivamente todos os aspectos do projeto, desde a reengenharia de processos até o projeto, desenvolvimento e otimização do sistema. A instituição está disponível para avaliar as necessidades de gerenciamento de mudança da organização e desenvolver o treinamento mais e caz para garantir a adoção total dos novos processos e tecnologia.

A empresa combina experiência com experiente pro ssionais na área de TI e análise de dados para fornecer soluções de software e cazes que podem automatizar e otimizar processos de negócios no prazo e dentro do orçamento.

Os analistas da organização desenvolveram várias ferramentas de análise de valor agregado para problemas reais do dia-a-dia. Mais importante ainda, os pro ssionais

testam e executam essas soluções em grandes quantidades de dados reais de algumas das empresas que tem contrato e obtém benefícios de negócios tangíveis e mensuráveis.

Os pro ssionais de tecnologia são atribuídos a cada projeto de cada cliente. As equipes são dinâmicas – as pessoas são designadas ou removidas da equipe de acordo com a fase e a carga de trabalho do projeto. Uma equipe pode consistir de 4 a 30 membros.

Para cada cliente, uma infraestrutura separada e concreta é criada. Esta infraestrutura inclui:

a) Um repositório de código centralizado, um arquivo de código quepermite a projetos de vários desenvolvedores lidar com várias versões;

b) Uma biblioteca de documentos centralizada;

c) Um diretório dedicado em uma ferramenta de gerenciamento deprojetos – listas de distribuição dedicadas;

d) Pro ssionais dedicados ao desenvolvimento e teste;

e) Um rastreador de problemas para o projeto – uma entrada separadapara uma ferramenta de gerenciamento de tempo.

As ferramentas e a infraestrutura descritas acima fornecem à equipe a estrutura apropriada para criar, gerenciar e entregar o projeto, a base de colaboração, as métricas e análises para a garantia de qualidade.

4.2 Situação da Empresa Antes da Implementação da Norma ISO 27001

Era uma política analisada que as informações que gerencia, tanto em formato eletrônico quanto em papel, fossem adequadamente protegidas para proteger contra as consequências de violações de con dencialidade, falhas de integridade ou interrupções na disponibilidade dessas informações.

A empresa já tinha muitos processos implementados. No entanto, a maioria deles não foi registrada regularmente ou de forma alguma. Ou seja, muitas das ameaças não foram identi cadas, portanto, não foram levadas em consideração.

Foram realizados treinamentos anuais e de integração sobre Segurança da Informação para conscientizar os funcionários sobre a política percebida em relação à segurança da informação. Uma equipe de segurança da informação já foi estabelecida. Os membros foram treinados e todos os membros da equipe puderam tratar de quaisquer questões relacionadas à Segurança da Informação.

Diante do exposto, a organização já possuía alguns processos estabelecidos que facilitariam o processo de atendimento à ISO 27001; no entanto, também havia muitas ameaças e vulnerabilidades que não foram identi cadas.

O rápido crescimento da organização revelou que o modelo de segurança da informação padronizado poderia tornar alguns aspectos do negócio mais funcionais. Além disso, cou claro que o rápido crescimento tornaria a empresa um alvo de ameaças cibernéticas e isso se tornou uma meta por si só para se prosseguir com uma política de Segurança da Informação mais detalhada e aprimorada.

A forma estabelecida de processar a segurança da informação não era sustentável. Os riscos decorrentes de erro humano se multiplicariam à medida que a força de trabalho cresce.

Por m, a empresa continuou recebendo a mesma pergunta de inúmeros clientes: “Por que devemos con ar nossas informações a você? ”. Com o passar dos anos, tornou-se cada vez mais desa ador voltar aos clientes com uma prova bem documentada. Além disso, os clientes tornaram-se cada vez menos tolerantes com a incerteza da segurança da informação e a equipe de segurança da informação não conseguia mais responder às necessidades dos clientes.

Portanto, tendo uma situação de segurança da informação que se mostra insustentável, a organização decidiu realizar a implementação de um SGSI com base na ISO/IEC 27001 e

garantir a sua certi cação, para ter uma maior con abilidade de seus clientes, além de garantir a integridade dos dados e informações que tinham.

4.3 Processo para Implementação da ISO 27001

Para a implementação da ISO 27001, o primeiro passo foi determinar a forma de implementar o processo de atendimento da norma e garantia da certi cação, dessa forma, foi utilizado o método PDCA com o ciclo:
Planejar (Plan) – Fazer (Do) – Veri car (Check) – Agir (Act):

. Planejar – Estabelecer SGSI: estabelecer uma política de segurança e procedimentos e controles relevantes; em seguida, preparar uma declaração do escopo de sua aplicação, justi cando porque os controles foram selecionados e outros não (SIPONEN; WILLISON, 2009). Estabelecer o SGSI, é identi car os ativos, requisitos, avaliar riscos e controlar a seleção.

. Fazer – Implementar SGSI: implementar a política de segurança e procedimentos relevantes (SIPONEN; WILLISON, 2009). Implementar o SGSI, determinar implementar os controles selecionados e gerenciar as operações.

. Veri car – Monitorar e revisar o SGSI: avaliar e medir o desempenho do processo e relatar os resultados para a gestão (SIPONEN; WILLISON, 2009). Monitorar e analisar o SGSI, caracteriza o levantamento de dados sobre o despenho para análise e avaliação.

. Agir – Manter e melhorar o SGSI: tomar as ações corretivas adequadas (SIPONEN; WILLISON, 2009). Manter e melhorar o SGSI, realiza a imposição de ações corretivas e preventivas para garantir o seu funcionamento de modo adequado a atingir os propósitos determinados nas políticas iniciais.

4.4 Avaliação de Risco e Tratamento de Risco

Como descrito previamente, risco é o impacto negativo de qualquer vulnerabilidade e ameaça que possa surgir nos sistemas de informação e ativos. A gestão de riscos permite identi car, avaliar e tomar as medidas e ações necessárias de forma sistemática para reduzir os riscos a um nível aceitável.

Dessa forma, a avaliação de risco, tratamento de risco e seus controles e

processos de suporte devem ser aplicados a todos os setores e departamentos, em relação a todos os riscos informativos e operacionais para todos os ativos que podem ser usados dentro da organização e / ou podem ter um impacto na segurança da informação. É aplicável a todas as avaliações de risco de segurança da informação conduzidas no escopo do Sistema de Gerenciamento de Segurança da Informação (SGSI) da empresa, incluindo todos os processos e ativos de negócios. A política de avaliação de risco e tratamento de risco se aplica também a todas as entidades comerciais da empresa (por exemplo, funcionários, parceiros, contratados, parceiros de entrega locais, fornecedores, membros do público).

4.4.1 Contexto Comercial e Técnico

A empresa estabeleceu o contexto comercial e técnico do sistema de informação que está sendo avaliado e garantiu que os objetivos do negócio sejam capturados, com todos os fatores internos e externos que in uenciam os riscos identi cados.

1) Contexto de negócios: Identi cação do proprietário de negócios dosistema de informação sendo revisado, classi cação de informações, processos de negócios suportados, usuários do sistema, requisitos de segurança e conformidade.

2) Contexto técnico: Identi cação do proprietário do serviço do sistema deinformação sendo revisado, usuários para apoiar e manter o sistema de informação, arquitetura lógica, componentes do sistema.

4.4.2 Processo de Avaliação de Risco

A avaliação de risco considera o valor dos sistemas de informação e ativos da organização. Se os objetivos de um ativo são críticos para as necessidades de negócios ou se os ativos são conhecidos por estarem em alto risco, uma avaliação de risco detalhada é conduzida para este ativo de informação especí co. Isso envolve a identi cação e validação aprofundadas de ativos, incluindo avaliação do impacto comercial de vulnerabilidades e ameaças a esses ativos.

A avaliação de risco realizada determinou identi car, quanti car e priorizar os riscos de acordo com os objetivos da empresa e assim de niu os critérios do nível aceitável de risco. Os resultados da avaliação de risco orientam a gestão na escolha das ações apropriadas e a ordem de prioridade correspondente para a administração dos riscos de segurança da informação e para a implementação de mecanismos de controle apropriados para proteger contra esses riscos.

A avaliação de risco inclui a avaliação sistemática da escala dos e o processo de comparação do risco com os critérios de risco para a determinação da importância dos riscos. O processo de avaliação de risco é conduzido periodicamente para abordar mudanças nos requisitos de segurança e condições de risco (por exemplo, ativos, ameaças, vulnerabilidades, impactos e outras mudanças signi cativas) e é realizado de uma forma metódica capaz de produzir resultados comparáveis e recorrentes, várias vezes dependendo da parte e da criticidade da empresa ou dos sistemas de informação em análise.

Uma avaliação de risco deve ser realizada com acesso e compreensão de:

1) Processos de negócios.

2) O impacto relacionado ao risco nos ativos de negócios.

3) Os sistemas técnicos implementados, suportando as necessidades donegócio.

4) A legislação e os regulamentos aos quais a empresa está sujeita.

5) Avaliações atualizadas de vulnerabilidade e ameaças. Uma avaliação derisco deve ser realizada pelo menos:

Uma avaliação de risco deve ser realizada pelo menos:

1) Para cada novo sistema de processamento de informações;

2) Após a introdução de um novo ativo de informação;

3) Após modi cações em sistemas ou processos;

4) Modi cações que podem alterar a natureza das ameaças evulnerabilidades;

5) Quando não houve revisão por um período relativamente longo (porexemplo, três anos).

Para cada um dos riscos identi cados após a avaliação de risco, a gestão da empresa teve que decidir sobre o método de tratamento de risco apropriado. Possíveis opções de tratamento de risco incluem:

1) Implementar mecanismos de controle adequados para reduzir riscos;

2) Aceitação dos riscos se as condições e critérios para aceitação do riscoforem atendidos;

3) Evitar riscos, não permitindo ações que possam causar riscos;

4) Transferência de riscos relacionados a outras partes (por exemplo,seguradoras ou fornecedores).

A decisão de risco com mecanismos de controle apropriados envolve a seleção e implementação de mecanismos de controle em linha com os requisitos resultantes da avaliação de risco. Os mecanismos de controle escolhidos devem garantir que os riscos sejam reduzidos a um nível aceitável, levando em consideração:

1) Os requisitos e limitações das leis e regulamentos nacionais einternacionais;

2) Obrigações contratuais com clientes e fornecedores;

3) Requisitos e objetivos de negócios conforme descrito acima;

4) Requisitos e restrições operacionais;

5) Os custos de aplicação e controle operacional em relação aos riscos quesão diminuídos e os riscos remanescentes, dependendo dos requisitos e restrições da empresa;

6) A necessidade de equilibrar o investimento na implementação eoperação dos controles e os danos que podem surgir no caso de falha de segurança;

7) Melhores Práticas.

4.4.3 Ativos e Vulnerabilidades

A identi cação de todos os ativos da empresa é a fase inicial do processo de avaliação de risco, no âmbito do SGSI. Ativos incluem documentos em formato físico ou eletrônico, aplicativos e bancos de dados, equipamentos de TI, infraestrutura, pessoas, serviços externos e terceirizados. Além disso, a identi cação de ativos deve incluir os proprietários de cada ativo (pessoal responsável, unidade organizacional). A identi cação de vulnerabilidades e ameaças de cada ativo é a próxima etapa na metodologia de risco. Várias vulnerabilidades e ameaças podem estar associadas a cada ativo.

Foi considerado todas as vulnerabilidades potenciais, ameaças aplicáveis a um sistema especí co, sejam intrínsecas ou extrínsecas, naturais ou humanas, acidentais ou maliciosas. A Tabela 1 demonstra as ameaças identi cadas.

Tabela 1 – Identi cação das ameaças.

Categoria	**Ameaças**
Roubo	Roubo, Vandalismo
Erro de software	Erro de software
Erro de software	Malware
Erro de software	Acesso não autorizado
Interrupção	Falta de energia

Interrupção	Interrupção de telecomunicações
Erro de rede	Ataque de rede
Desastre natural	Tremor de terra
Desastre natural	Inundar
Desastre natural	Incêndio
Jurídico	Quebra de relações contratuais
Jurídico	Violação de legislação
Erro humano	Uso indevido de informação
Erro humano	Erro do operador
Erro humano	Uso indevido de privilégios de usuário
Erro humano	Destruição de registros
Erro de hardware	Erro de hardware
Erro de hardware	Danos ao cabeamento
Erro de acesso	Bloqueado
Erro de software	Erros na manutenção
Erro de hardware	Mau funcionamento do equipamento
Erro humano	Instalação não autorizada de software
Descarte de hardware	Exclusão não segura de mídia
Reutilização de hardware	Reatribuição não segura de hardware
Midia removivel	Uso de mídia removível não criptografada

Fonte: Próprio Autor (2025).

As informações de vulnerabilidade e ameaça que são detalhados na Tabela 1, foram obtidas dos usuários apropriados da empresa e, em alguns casos, de consultorias especializadas em segurança, serviços de segurança e contatos.

4.4.4 Identi cação dos Riscos

Os riscos relacionados aos sistemas de informação, informações e operações podem ser identi cados nas seguintes categorias:

1) Qualquer usuário identi ca ameaças que são relevantes para os ativossob análise;

2) Uma lista abrangente de eventos que podem impedir ou atrasar osobjetivos de negócios deve ser documentada. O risco não incluído nesta lista pode não ser avaliado e mitigado;

3) Ameaças de repositórios existentes podem ser adicionadas apóspesquisas relacionadas;

4) Descrição clara dos riscos, para serem analisados e avaliados;

5) A identi cação de risco deve incluir o impacto potencial nos sistemasde informação e ativos da empresa.

Qualquer risco potencial que possa afetar a con dencialidade, integridade e disponibilidade dos sistemas de informação, dados, operações e ativos da empresa será documentado no processo de avaliação de risco. Os critérios de avaliação de risco devem ser estabelecidos a m de fornecer um entendimento comum dessas medidas de segurança, o que minimizará o impacto potencial a um nível aceitável. O nível de dano e os custos causados por uma ameaça determinarão os critérios de impacto.

Os critérios de impacto são demonstrados na Tabela 2.

Tabela 2 – Critérios de impacto.

Critérios de Impacto

Perda de valor nanceiro	Consequências em procedimentos correlacionados
Consequências nanceiras diretas	Incidentes de segurança, ataques
Consequências nanceiras indiretas de longo prazo	Violações de requisitos legais e regulamentares
Perturbação de planos e prazos	Questões de contrato privado
Obstrução de procedimentos da empresa	Questões de privacidade
Perda de valor comercial	Questões relacionadas à competição
Perda de oportunidade	Dados con denciais e pessoais, danos à reputação
Falhas em atividades comerciais	Questões de con dencialidade pública

Fonte: Próprio Autor (2025).

4.4.5 Atividades de Avaliação de Risco

A m de determinar a probabilidade de um evento futuro e / ou ameaça que possa causar danos potenciais aos sistemas de informação e ativos da empresa, uma análise é conduzida com as vulnerabilidades identi cadas e os controles de segurança em vigor. O impacto da perda de

con dencialidade, integridade e disponibilidade é avaliado de acordo com os critérios de impacto. A probabilidade de ocorrência é um fator de risco em uma análise da probabilidade de que uma determinada ameaça seja capaz de explorar uma determinada

(ou um conjunto de) vulnerabilidade. O risco é o resultado da probabilidade de uma certa ameaça de uma vulnerabilidade potencial e o impacto resultante (probabilidade) nos sistemas de informação ou seus ativos.

As atividades de avaliação de risco fornecerão as informações necessárias para o desenho de controles e medidas de segurança apropriados que irão reduzir ou eliminar riscos, durante o processo de mitigação (tratamento de risco).

As etapas que levam à implementação de uma avaliação de risco incluem as seguintes atividades:

1) Identi cação da ameaça: A probabilidade de ocorrência de cadapossível ameaça é avaliada. A probabilidade de ameaça (nível de ameaça) é de nida como a frequência de aparecimento esperada. Ao determinar a probabilidade de uma ameaça, a empresa deve levar em consideração as fontes de ameaça, vulnerabilidades potenciais e controles existentes.

2) Identi cação de vulnerabilidade: a análise de uma ameaça a umsistema de informação deve incluir uma análise das vulnerabilidades associadas ao ambiente. Avaliando assim os níveis de vulnerabilidade em relação a um cenário de ameaça e aplicando e testando os controles.

3) Análise de controle: os controles implementados devem ser levados emconsideração e testados a m de minimizar e / ou eliminar a probabilidade de uma ameaça que surge de uma vulnerabilidade do sistema.

4) Determinação da probabilidade: A empresa deve considerar osseguintes fatores importantes: fonte de ameaça da vulnerabilidade (natureza), existência e e cácia dos controles atuais. A probabilidade de ocorrência que uma ameaça toma como entrada, o nível de ameaça e as saídas do nível de vulnerabilidade, além da probabilidade de ocorrência para a ameaça especí ca.

5) Análise de impacto: O impacto de um evento de segurança pode serdescrito em termos de – e / ou uma combinação de qualquer – perda de con dencialidade, integridade e disponibilidade.

6) Determinação do risco: A probabilidade de ocorrência e os valores deimpacto são combinados de forma a estimar o nível de risco de cada ativo, para uma ameaça identi cada. A adequação dos controles de segurança existentes e planejados também serão incluídos para avaliar o nível de risco.

7) Recomendação de controle: controles de segurança que podemmitigar e / ou eliminar os riscos identi cados, em alinhamento com as operações da empresa. Os controles recomendados devem assegurar que o nível de risco será reduzido a um nível aceitável.

8) Documentação de resultados: Após a conclusão da avaliação de risco,os resultados devem ser documentados em um relatório o cial.

Os níveis de risco são avaliados com critérios estabelecidos, e as medidas apropriadas deverão ser tomadas.

4.4.6 Avaliação de Probabilidade e Impacto

Em caso de risco, é necessário avaliar as consequências relevantes para cada vulnerabilidade e ameaça, para um ativo individual. A probabilidade de ocorrência de tal risco é necessária para ser avaliada para cada ativo da empresa. A gravidade de um risco é uma avaliação geral da probabilidade de acontecer (probabilidade) e do impacto, se acontecer (ocorrência do impacto), dessa forma, foram levantados todos os níveis possíveis como demonstrados na Tabela 3.

A probabilidade de uma vulnerabilidade e / ou ameaça potencial pode ser descrita como (Quase certa, Provável, Possível, Improvável, Rara). O impacto de um incidente de segurança pode ser descrito em termos de perda de con dencialidade, integridade e disponibilidade, todos os impactos a partir dos incidentes de segurança foram determinados e são descritos na Tabela 4.

Tabela 3 –Níveis de probabilidade.

Nível de Probabilidade	Descrição da probabilidade
Quase certo	Espera-se que ocorra na maioria das circunstâncias.
Provável	Provavelmente ocorrerá na maioria das circunstâncias.
Possível	Pode ocorrer em algum momento.
Improvável	Não esperado, mas concebível, pode ocorrer algum dia.
Raro	Não era esperado e ocorreria apenas em circunstâncias específicas.

Fonte: Próprio Autor (2025).

Tabela 4 – Níveis de impacto.

Nível de Impacto	Descrição do impacto
Alto (H5, H4, H3, H2, H1)	A perda de disponibilidade, confidencialidade ou integridade tem considerável, crítica e / ou impacto imediato no fluxo de caixa da empresa, operações, funcionalidade, obrigações legais, contratuais e / ou sua reputação.
Médio (M5, M4, M3, M2, M1)	A perda de confidencialidade, disponibilidade ou integridade pode causar custos e ter impacto médio ou baixo nas obrigações legais, contratuais e / ou na reputação da empresa.
Baixo (L5, L4, L3, L2, L1)	A perda de confidencialidade, disponibilidade ou integridade não afeta o fluxo de caixa da empresa, obrigações legais, contratuais e / ou sua reputação.

Fonte: Próprio Autor (2025).

4.4.7 Matriz de Riscos

A empresa desenvolveu uma escala de risco e uma matriz de risco para medir um risco identi cado. A determinação nal do risco é derivada da multiplicação da classi cação atribuída para a probabilidade da ameaça e o impacto da ameaça. As classi cações gerais de risco podem ser determinadas com base nas informações das categorias de probabilidade de ameaça e impacto de ameaça.

A matriz com os níveis de risco (Tabela 5) é uma matriz 5 x 15 de probabilidade de ameaça (quase certa, provável, possível, improvável, rara) e impacto de ameaça (alto 1-5, médio 1-5, baixo 1-5) e mostra como os níveis gerais de risco são derivados. A determinação desses níveis ou classi cações de risco pode ser subjetiva. A justi cativa para essa explicação pode ser demonstrada em termos da probabilidade atribuída para cada nível de probabilidade de ameaça e um valor atribuído para cada nível de impacto. Para cada ativo da empresa, todas as ameaças possíveis serão atribuídas. A escala de classi cação para os níveis de impacto (em termos de con dencialidade, integridade e

disponibilidade) é de nida como uma escala de classi cação de 15 pontos de L1 a H5: L1, L2, L3, L4, L5, M1, M2, M3, M4, M5, H1, H2, H3, H4, H5. A escala de avaliação dos níveis de probabilidade é de nida como uma escala de avaliação de 5 pontos: Raro: 0,20, Improvável: 0,40, Possível: 0,60, Provável: 0,80, Quase certo: 1,00. O limite de risco é de nido em 2,9.

A matriz risco com suas classi cações representa o nível de risco ao qual o sistema de informação, ativo e / ou processo pode ser exposto dada uma vulnerabilidade identi cada, ameaça.

Tabela 5 – Matriz de risco.

			Probabilidade				
			Raro	Improvável	Possível	Provável	Quase Certo
		Valor	0,20	0,40	0,60	0,80	1,00
Impacto	H5	15	3	6	9	12	15
	H4	14	2,8	5,6	8,4	11,2	14
	H3	13	2,6	5,2	7,8	10,4	13
	H2	12	2,4	4,8	7,2	9,6	12
	H1	11	2,2	4,4	6,6	8,8	11
	M5	10	2	4	6	8	10
	M4	9	1,8	3,6	5,4	7,2	9
	M3	8	1,6	3,2	4,8	6,4	8
	M2	7	1,4	2,8	4,2	5,6	7
	M1	6	1,2	2,4	3,6	4,8	6
	L5	5	1	2	3	4	5
	L4	4	0,8	1,6	2,4	3,2	4
	L3	3	0,6	1,2	1,8	2,4	3
	L2	2	0,4	0,8	1,2	1,6	2
	L1	1	0,2	0,4	0,6	0,8	1

Fonte: Próprio Autor (2025).

Tabela 6 – Relação da probabilidade e consequências.

Avaliação de probabilidade	Menor	Sério	Severo	Maior	Catastrófico
Quase certo	Médio	Alto	Crítico	Crítico	Crítico
Provável	Médio	Significativo	Alto	Crítico	Crítico
Possível	Médio	Médio	Significativo	Alto	Crítico
Improvável	Baixo	Baixo	Médio	Significativo	Crítico
Raro	Baixo	Baixo	Médio	Médio	Alto

Fonte: Próprio Autor (2025).

Tabela 7 – Níveis de consequência.

Crítico	Risco extremo - pesquisa detalhada, planejamento de gestão necessário
Alto	Alto risco - atenção imediata necessária
Significativo	Risco significativo - atenção de gerenciamento necessária
Médio	Risco médio - a responsabilidade de gestão deve ser especificada
Baixo	Baixo risco - procedimentos de rotina devem ser gerenciados

Fonte: Próprio Autor (2025).

4.4.8 Tratamento do Risco

Para cada risco identi cado, uma resposta deve ser determinada. A probabilidade e o impacto do risco serão a base para recomendar quais ações devem ser tomadas para mitigar o risco. Uma opção de tratamento (controles de segurança) deve ser identi cada de acordo com a análise de custo-benefício e os critérios de impacto relevantes. O tratamento de risco consiste nos seguintes quatro níveis:

1) Aceitar: A aceitação do risco normalmente só deve ser feita para riscosde baixa prioridade, nos casos em que outras opções de tratamento custarão mais do que o impacto potencial. Todos os riscos devem ter recomendação de controle (s) e soluções alternativas para mitigar o risco identi cado. A empresa aceitará o risco identi cado.

2) Redução: a mitigação de risco envolve a redução da probabilidade e /ou impacto da ameaça / vulnerabilidade de risco a um nível aceitável. A ação pró-ativa contra o risco costuma ser mais e caz do que tentar reparar o dano causado por um risco identi cado. A empresa planejará e projetará controles futuros para lidar com o risco identi cado.

3) Transferência: a transferência de risco envolve a mudança do impactonegativo de uma ameaça, a vulnerabilidade. Transferir o risco para terceiros (fornecedores) não elimina uma ameaça, vulnerabilidade. Outra parte será responsável por gerenciar o risco relacionado. A empresa irá listar todas as opções para os riscos identi cados, a m de serem transferidos para outras entidades (por exemplo, seguro).

4) Remoção: a prevenção de riscos envolve a mudança de aspectos dosprocessos gerais de negócios ou da arquitetura do sistema para eliminar a ameaça e a vulnerabilidade. Evitar o risco ao interromper a atividade comercial relacionada. A empresa planejará todas as ações apropriadas para a remoção de ativos relacionados aos riscos identi cados.

Para cada ativo por ameaça, deverá ser avaliado seu impacto e níveis de probabilidade. Quando o nível de risco está acima do limite de risco, a empresa deve examinar todos os controles no local. Uma nova revisão dos níveis de risco será realizada e, de acordo com o novo nível de risco, uma ação de tratamento de risco deverá ser avaliada. As opções de tratamento devem ser documentadas para cada risco identi cado.

4.4.9 Seleção de Controles

Os objetivos de controle apropriados são selecionados a m de mitigar os riscos identi cados e minimizar o impacto potencial nos sistemas de informação da empresa. Os controles de segurança são selecionados e / ou projetados de acordo com os controles do Anexo da ISO / IEC 27001: 2013 para garantir que nenhum foi esquecido. Os controles selecionados para suas respectivas ameaças serão documentados.

4.4.10 Plano de Tratamento de Risco

Um plano de tratamento de riscos é estabelecido a m de gerenciar e mitigar as ações de remediação necessárias. O plano de tratamento de risco é projetado para reduzir os riscos aos ativos críticos da empresa. Qualquer risco potencial que possa surgir de vulnerabilidades e ameaças identi cadas deve ser tratado de acordo com seu nível de consequência.

A gestão da empresa, em consulta com os proprietários do risco, aceita todos os riscos restantes, em conformidade. O plano de tratamento de risco será preparado pelo Diretor de Segurança da Informação, onde o projeto e a implementação dos controles serão programados.

4.4.11 Responsabilidades

O Diretor de Segurança da Informação monitorará o progresso da implementação do plano de tratamento de risco regularmente e a e cácia da estrutura de segurança da informação para garantir que os controles de segurança relacionados sejam e cazes conforme projetado. Os resultados e as análises subsequentes da avaliação de risco e do tratamento de risco serão documentados. O Diretor de Segurança da Informação deve atualizar a avaliação de risco e o risco residual correspondente em conformidade.

O Gerente de Segurança da Informação é responsável por realizar avaliações de risco sempre que exigido pelo SGSI da empresa e em coordenação com o Diretor de Segurança da Informação. Além disso, o
Gerente de Segurança da Informação, em colaboração com os
Proprietários dos Dados da Informação, revisará os riscos médios e baixos e recomendará as ações adequadas. O Gerente de Segurança da Informação também é responsável por manter canais de comunicação com os especialistas apropriados.

4.4.12 Análise do Processo

A gestão de risco é um processo na estrutura do Sistema de Gestão de Segurança da Informação (SGSI) com a intenção de contribuir para a identi cação, avaliação e tratamento sistemático dos riscos e para garantir um nível aceitável de segurança da informação dentro do escopo do SGSI.

Com base nesse contexto o presente estudo realizado, demonstrou a caracterização da avaliação de risco e tratamento de risco no contexto da segurança da informação, tendo como propósito e objetivo: Identi cação precoce, gestão e tratamento de riscos de forma tolerada e aceitável;
Estabelecimento de métodos consistentes de identi cação de riscos;

Atribuição clara de responsabilidades quando os riscos são identi cados; Documentação clara dos riscos com sua avaliação; Implementação de melhores controles de segurança nos sistemas de informação; Melhores decisões de avaliação de risco, fornecendo informações para controles de segurança econômicos; Projetar controles físicos, procedimentais e técnicos acordados com os proprietários dos ativos de informação; Tratamento e ciente de riscos.

Embora existam muitas abordagens diferentes sobre como implementar com sucesso um SGSI em uma empresa, o resultado desejado é o mesmo: manter as informações seguras e encontrar a solução ideal que cubra as necessidades da organização. Mesmo assim, o presente estudo seguiu e caracterizou todos os processos relacionados a associados a ISO/IEC 27001.

Todos os processos de implementação das medidas apresentadas foram acompanhados junto com a equipe de implantação da ISO 27001, a implantação de uma estratégia de prevenção de vazamento de informações con denciais é algo vital para a organização.

Um grande número de ameaças exigiu atenção e cuidado da equipe. Muitos controles foram aplicados para mitigar todas as ameaças e resultados para o tratamento do risco; quais ameaças precisavam ser transferidas, aceitas e removidas. No entanto, a empresa não passou pela auditoria externa e, portanto, pelo processo de certi cação até a nalização do processo de implementação das medidas apresentadas.

Este estudo de caso apresentado foi o resultado da longa jornada de implantação da ISO 27001 de uma empresa de TI. A avaliação de risco e o

tratamento de risco levaram mais de 11 meses e 16 versões para serem concluídos. Isso acrescentou complexidade e atraso não apenas aos processos, mas também a algumas atividades exercidas pela própria instituição.

5. Conclusão

A implementação de um Sistema de Gestão de Segurança da Informação

(SGSI) com base na norma ISO/IEC 27001, como detalhado neste estudo, demonstrou ser uma estratégia essencial para fortalecer a proteção dos ativos de informação e assegurar a continuidade operacional da organização analisada. A metodologia adotada, pautada pelo ciclo PDCA, permitiu um processo estruturado e e ciente, abrangendo desde a identi cação de ativos críticos e avaliação de riscos até a de nição de controles especí cos e monitoramento contínuo.

Os resultados evidenciam que, apesar dos desa os enfrentados, como a complexidade no mapeamento de vulnerabilidades e a necessidade de engajamento contínuo da equipe, a adoção da norma ISO 27001 trouxe benefícios expressivos à organização. Destaca-se o aumento da resiliência frente a ameaças cibernéticas, a melhoria na percepção de con abilidade por parte dos clientes e a consolidação de uma cultura organizacional voltada à segurança.

Ademais, a análise de risco revelou a importância de uma abordagem preventiva e integrada, que não apenas minimiza os impactos potenciais, mas também orienta a alocação e ciente de recursos e a priorização de ações corretivas. A matriz de riscos desenvolvida e o plano de tratamento de risco elaborado demonstraram-se ferramentas e cazes para a gestão proativa dos riscos, promovendo a conformidade com requisitos regulatórios e contratuais.

Em termos técnicos, a implementação de controles de segurança robustos e a adoção de tecnologias avançadas, como criptogra a e autenticação multifatorial, destacaram-se como pilares fundamentais para a mitigação de riscos. No entanto, o sucesso do SGSI também dependeu de fatores humanos, como a conscientização e o treinamento dos colaboradores, reforçando a necessidade de uma abordagem holística na gestão da segurança da informação.

Conclui-se que, embora a certi cação formal ainda não tenha sido obtida, o processo de implementação do SGSI já resultou em melhorias signi cativas na governança da informação e na capacidade de resposta a incidentes. Este estudo de caso contribui para a literatura ao oferecer uma visão detalhada e prática dos desa os e soluções associados à implementação da norma ISO/IEC 27001, servindo como referência para organizações que buscam aprimorar sua postura de segurança.

Como recomendações para trabalhos futuros, sugere-se a investigação de modelos híbridos de segurança da informação, que integrem padrões complementares à ISO 27001, bem como a análise comparativa do impacto econômico pós-certi cação em diferentes setores. Além disso, a realização de auditorias periódicas e a atualização contínua do SGSI são essenciais para garantir a e cácia e a aderência às melhores práticas, diante de um cenário de ameaças em constante evolução.

REFERÊNCIAS

CALDER, A. **Information security based on ISO 27001/ISO 27002: a management guide – best practice**, 2009.

CALDER, Alan; WATKINS, Steve. **IT Governance:** An International Guide to Data Security and ISO27001/ISO27002. 6. ed. London: Kogan Page, 2021.

CASACA, Joaquim A.; CORREIA, Manuela Faia. **Porque é necessária a segurança da informação? Da estratégia às políticas de segurança**.
Lisboa, 2013.

CISSE, M. **An ISO 27001 compliance project for a cyber security service team**. Cyber Security: A Peer-Reviewed Journal, 2019.

DISTERER, G. **ISO/IEC 27000, 27001 and 27002 for information security management**. Journal of Information Security, 2013.

DOHERTY, Neil F.; FULFORD, Helen. **Information Security Policy:** A Development Guide for Large and Small Companies. New York:
Routledge, 2013.

EWUGA, S. K.; EGIEYA, Z. E.; OMOTOSHO, A.; ADEGBITE, A. O. **ISO 27001 in banking: an evaluation of its implementation and effectiveness in enhancing information security**. Finance & Accounting Research Journal, 2024.

FRANCO, Deivison Pinheiro. **Gestão de conhecimento para segurança da informação**. 2014.

GORDON, Lawrence A.; LOEB, Martin P. **Managing Cybersecurity Resources:** A Cost-Bene t Analysis. Boston: Springer, 2015.

GUALBERTO, E. S.; DEUS, F. **Proposição de uma ontologia de apoio à gestão de riscos de segurança da informação**. 2013.

GUO, H.; WEI, M.; HUANG, P.; CHEKOLE, E. G. **Enhance enterprise security through implementing ISO/IEC 27001 standard**. 2021 IEEE International
Conference on Service Operations and Logistics, and Informatics (SOLI), 2021.

MARCIANO, J.; LIMA-MARQUES, Mamede. **O enfoque social da segurança da informação**. 2006.

MILITARU, C. Human resources security management towards ISO/IEC 27001:2005 accreditation of an information security management system, 2009.

MORAES, J. P.; SAGAZ, Sidimar Meira; SANTOS, Genéia Lucas dos; LUCIETTO, D. Tecnologia da informação, sistemas de informações gerenciais e gestão do conhecimento com vistas à criação de vantagens competitivas: revisão de literatura. 2017.

NORTHCUTT, Stephen. **Network Security Monitoring**. 2. ed. Indianapolis:
Pearson IT Certi cation, 2014.

OLIVEIRA, L. A. D.; FELIPE, I. **Sistema de gestão ambiental: um diferencial estratégico competitivo na gestão de processos produtivos**.
2013.

PELTIER, Thomas R. **Information Security Risk Analysis**. 3. ed. New York:
Auerbach Publications, 2016.

PEREIRA, Samáris Ramiro et al. **Segurança na arquitetura de sistemas informatizados**. 2011.

PUTRA, D. S. K.; TISTIYANI, S.; SUNARINGTYAS, S. U. **The use of ISO/IEC 27001 family of standards in regulatory requirements in some countries**. 2021 2nd International Conference on ICT for Rural Development (IC-ICTRuDev), 2021.

ROSS, Ron; MCELREATH, David; et al. **NIST Special Publication 800-37:**
Guide for Applying the Risk Management Framework to Federal Information Systems. Washington, DC: NIST, 2018.

SANTOS, Erika Alves dos; MIRAGLIA, Simone Georges El Khouri. **Arquivos abertos e instrumentos de gestão da qualidade como recursos para a disseminação da informação cientí ca em segurança e saúde no trabalho**. 2018.

SCHNEIER, Bruce. **Applied Cryptography:** Protocols, Algorithms, and Source Code in C. 20. ed. New York: John Wiley & Sons, 2015.

SHARMA, N.; DASH, P. K. **Effectiveness of ISO 27001, as an information security management system: an analytical study of nancial aspects**.
The Far East Journal of Psychology and Business, 2012.

SILVA, L. Sistemas de informações em saúde como ferramenta para gestão do SUS. 2016.

STALLINGS, William. **Cryptography and Network Security:** Principles and Practice. 8. ed. New York: Pearson, 2020.

TIPTON, Harold F.; KRAUSE, Micki. **Information Security Management Handbook**. 7. ed. Boca Raton: CRC Press, 2012.

UKIDVE, A.; TADVALKAR, M. **Analysis of management of information security and related enterprise risks in view of ISO/IEC 27001:2013**. Journal of Emerging Trends in Economics and Management Sciences, 2016.

VAKHULA, O.; KURII, Y.; OPIRSKYY, I.; SUSUKAILO, V. **Security as code** concept for ful lling ISO/IEC 27001: 2022 requirements, 2024.

VIEIRA, F. S. **Produção de informação de custos para a tomada de decisão no Sistema Único de Saúde: uma questão para a política pública**. 2017.

WHITMAN, Michael E.; MATTORD, Herbert J. **Principles of Information Security**. ed. Boston: Cengage Learning, 2019.

---

[1]Discente do Curso Superior de Tecnologia em Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia do Amapá (IFAP) – Campus Macapá. E- mail: Carlos.lho10@gmail.com

[2]Docente do Curso Superior de Tecnologia em Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia do Amapá (IFAP) – Campus Macapá. Tecnólogo em Sistemas para Internet (META). E-mail: Andrew.rodrigues@ifap.edu.br

← Post anterior Post seguinte →

ISSN: 1678-0817

CNPJ: 48.728.404/0001-22

FI= 5.397 (muito alto)

Fator de impacto determinado é um método bibliométrico para avaliar a importância de periódicos científicos em suas respectivas áreas. Uma medida que reflete o número médio de citações de artigos científicos publicados em periódico, criado por Eugene Garfield, em que os de maior FI são considerados mais importantes.

Rua José Linhares, 134 - Leblon | Rio de Janeiro-RJ | Brasil