FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Pedro Israel Arissa Domingos dos Santos

APLICAÇÃO DE CONTROLES BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

Impacto no aumento do nível de maturidade de uma microempresa

Americana, SP

2025

FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Pedro Israel Arissa Domingos dos Santos

APLICAÇÃO DE CONTROLES BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

Impacto no aumento do nível de maturidade de uma microempresa

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação sob a orientação do Prof.(o) Me. Edson Roberto Gaseta

Área de concentração: segurança da informação.

Americana, SP

2025

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi- CEETEPS
Dados Internacionais de Catalogação-na-fonte

SANTOS, Pedro Israel Arissa Domingos dos

Aplicação de controles básicos de segurança da informação: impacto no aumento do nível de maturidade de uma microempresa. / Pedro Israel Arissa Domingos dos Santos – Americana, 2025.

44f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Edson Roberto Gaseta

1. Segurança em sistemas de informação. I. SANTOS, Pedro Israel Arissa Domingos dos II. GASETA, Edson Roberto III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681.518.5

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Pedro Israel Arissa Domingos Dos Santos

APLICAÇÃO DE CONTROLES BÁSICOS DE SEGURANÇA DA INFORMAÇÃO Impacto no aumento do nível de maturidade de uma microempresa

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana Ministro Ralph Biasi.
Área de concentração: Segurança da Informação

Americana, 26 de junho de 2025.

Banca Examinadora:

Edson Roberto Gaseta
Mestre
Fatec Americana "Ministro Ralph Biasi"

Benedito Aparecido Cruz
Mestre
Fatec Americana "Ministro Ralph Biasi"

Tiago Rebecca
Mestre
Fatec Americana "Ministro Ralph Biasi"

Agradeço aos professores do Curso de Tecnologia em Segurança da Informação pelo conhecimento transmitido durante todo o curso, em especial ao professor Gaseta pela orientação neste trabalho. Também agradeço aos colegas Luciana, Rafael e Thiago pela amizade e parceria durante o curso. Por fim, agradeço minha companheira Camila por ter me apoiado e suportado nos últimos três anos.

RESUMO

Este trabalho de conclusão de curso propõe-se a demonstrar a influência da aplicação de controles básicos de segurança da informação no nível de maturidade de microempresas. O estudo justifica-se pela crescente digitalização dos negócios, o surgimento de novos pequenos empreendimentos e a regulamentação sobre o tratamento de dados pessoais no Brasil, como a Lei Geral de Proteção de Dados (LGPD), que impõem desafios significativos para empresas com recursos limitados em segurança. O objetivo principal é investigar como pequenas empresas podem mitigar riscos e melhorar seu cenário de proteção de dados por meio de implementações simples de segurança.

A pesquisa, de natureza exploratória, combinou revisão bibliográfica sobre conceitos como controles de segurança da informação, risco e nível de maturidade, com uma análise da influência desses controles na maturidade da segurança da informação. Foram utilizados frameworks de gestão de segurança da informação, como o COBIT e o CIS Controls, para fundamentação e para a matriz de maturidade. A hipótese central é que a implementação de controles básicos tem um impacto significativo no nível de maturidade de segurança de uma microempresa. O objeto da pesquisa foi uma microempresa do setor de comunicação.

Os resultados deste trabalho contribuem para ampliar o escopo de estudos sobre estratégias acessíveis de segurança para pequenas empresas, fornecendo um caminho para o aprimoramento da proteção de dados e informações cruciais em um ambiente digital cada vez mais propenso a riscos.

Palavras-chave: segurança da informação, nível de maturidade, pequenas empresas.

ABSTRACT

This project investigates the influence of applying basic information security controls on the maturity level of microenterprises. The study is justified by the rapid digitalization of businesses, the proliferation of new small businesses, and the emergence of personal data protection regulations in Brazil, such as the General Data Protection Law (LGPD), which pose significant security challenges for resource-constrained companies. The primary objective is to demonstrate how small businesses can mitigate risks and enhance their data protection posture through simple security implementations.

The research employs an exploratory approach, combining a literature review on concepts such as information security controls, risk, and maturity level, with a analysis of how these controls can influence information security maturity. Information security management frameworks, including COBIT and CIS Controls, were utilized for theoretical grounding and for defining the security maturity matrix. The central hypothesis posits that the application of basic information security controls significantly impacts a microenterprise's security maturity level. The subject of this research was a microenterprise operating in the communication sector.

The findings of this work contribute to expanding the body of studies on accessible security strategies for small businesses, providing a pathway for improving data and critical information protection in an increasingly risk-prone digital environment

Keywords: *information security, maturity level, small businesses.*

LISTA DE ILUSTRAÇÕES

Figura 1 - Classificação de níveis de maturidade do framework COBIT. 19
Figura 2 - Situação geral da organização quanto aos controles existentes no CIS Controls. 23
Figura 3 - Nível de maturidade do controle 1 da organização antes das medidas propostas pelo estudo de caso.....24
Figura 4 - Nível de maturidade do controle 2 da organização antes das medidas propostas pelo estudo de caso.....25
Figura 5 - Nível de maturidade do controle 3 da organização antes das medidas propostas pelo estudo de caso.....26
Figura 6 - Nível de maturidade do controle 4 da organização antes das medidas propostas pelo estudo de caso.....28
Figura 7 - Nível de maturidade do controle 5 da organização antes das medidas propostas pelo estudo de caso.....30
Figura 8 - Nível de maturidade do controle 6 da organização antes das medidas propostas pelo estudo de caso.....31
Figura 9 - Nível de maturidade do controle 7 da organização antes das medidas propostas pelo estudo de caso.....33
Figura 10 - Nível de maturidade do controle 8 da organização antes das medidas propostas pelo estudo de caso.....34
Figura 11 - Nível de maturidade do controle 9 da organização antes das medidas propostas pelo estudo de caso.....35
Figura 12 - Nível de maturidade do controle 10 da organização antes das medidas propostas pelo estudo de caso.....35
Figura 13 - Nível de maturidade do controle 11 da organização antes das medidas propostas pelo estudo de caso.....36
Figura 14 - Nível de maturidade do controle 12 da organização antes das medidas propostas pelo estudo de caso.....37
Figura 15 - Nível de maturidade do controle 14 da organização antes das medidas propostas pelo estudo de caso.....38
Figura 16 - Nível de maturidade do controle 15 da organização antes das medidas propostas pelo estudo de caso.....38

Figura 17 - Nível de maturidade do controle 17 da organização antes das medidas propostas pelo estudo de caso.....39

LISTA DE ABREVIATURAS E SIGLAS

PNAD: Pesquisa Nacional de Amostra de Domicílios

IBGE: Instituto Brasileiro de Geografia e Estatística

SEBRAE: Serviço Brasileiro de Apoio às Micro e Pequenas Empresas

LGPD: Lei Geral de Proteção de Dados

CIS: Center for Internet Security

SSH: *Secure Shell*

HTTPS: *HyperText Transfer Protocol Secure*

AMF: Autenticação multi fator

SPF: *Sender Policy Framework*

DKIM: *DomainKeys Identified Mail*

DMARC: *Domain-based Message Authentication, Reporting and Conformance*

SUMÁRIO

INTRODUÇÃO **13**
1 FUNDAMENTAÇÃO TEÓRICA **15**
1.1 Controles de segurança da informação **15**
1.2 Risco em segurança da informação **15**
1.3 Maturidade em segurança da informação **16**
1.4 Governança em segurança da informação **17**
1.4.1 COBIT ---------- 18
1.4.2 CIS *Controls* ---------- 19
1.4.3 Mapeamento de controles do CIS Controls e da Norma Brasileira ABNT NBR ISO/IEC 27002---------- 20
2 METODOLOGIA **22**
3 ESTUDO DE CASO **23**
3.1 Apresentação da empresa **23**
3.2 Grupo de implementação **24**
3.3 Controles e salvaguardas **24**
3.3.1 Controle 1: inventário e controle de ativos empresariais ---------- 24
3.3.1.1 Estabelecer e manter inventário detalhado de ativos empresariais 24
3.3.1.2 Endereção ativos não autorizados 25
3.3.2 Controle 2: inventário e controle de ativos de *software* ---------- 25
3.3.2.1 Estabelecer e manter um inventário de software 25
3.3.2.2 Garantir que o software autorizado receba suporte 26
3.3.2.3 Endereçar software não autorizado 26
3.3.3 Controle 3: proteção de dados---------- 26
3.3.3.1 Estabelecer e manter um processo de gerenciamento de dados ... 27
3.3.3.2 Estabelecer e manter um inventário de dados 27
3.3.3.3 Configurar listas de controles de acesso a dados 27
3.3.3.4 Aplicar retenção de dados 27
3.3.3.5 Descartar dados de forma segura 28
3.3.3.6 Criptografar dados em dispositivos de usuários 28
3.3.4 Controle 4: configuração segura de ativos de *software* empresariais--- 28
3.3.4.1 Estabelecer e manter um processo de configuração segura 28

3.3.4.2 Estabelecer e manter configuração segura da infraestrutura de rede 29
3.3.4.3 Configurar bloqueio automático de sessão 29
3.3.4.4 Implementar e gerenciar firewall em servidores 29
3.3.4.5 Implementar firewall em dispositivos de usuário final 29
3.3.4.6 Gerenciar de forma segura ativos e software da empresa 29
3.3.5 Controle 5: gerenciamento de contas ---------- 29
3.3.5.1 Estabelecer e manter inventário de contas 30
3.3.5.2 Utilizar senhas únicas 30
3.3.5.3 Desativar contas inativas 30
3.3.5.4 Restringir privilégio de administrador a contas dedicadas 31
3.3.6 Controle 6: gerenciamento de controle de acesso ---------- 31
3.3.6.1 Estabelecer processo de concessão de acessos 31
3.3.6.2 Estabelecer processo de revogação de acessos 32
3.3.6.3 Exigir AMF para aplicações expostas externamente 32
3.3.6.4 Exigir AMF para acesso remoto ao ambiente corporativo 32
3.3.6.5 Exigir AMF para acesso administrativo 32
3.3.7 Controle 7: gerenciamento contínuo de vulnerabilidades ---------- 32
3.3.7.1 Estabelecer e manter um processo de gerenciamento de vulnerabilidades 33
3.3.7.2 Remediar vulnerabilidades 33
3.3.8 Controle 8: gerenciamento de logs de auditoria ---------- 33
3.3.8.1 Ativar e configurar logs de auditoria 34
3.3.8.2 Revisar logs de auditoria 34
3.3.9 Controle 9: proteção de *e-mail* e navegador *web* ---------- 34
3.3.9.1 Configurar proteção de e-mail 35
3.3.9.2 Configurar proteção de navegadores 35
3.3.10 Controle 10: proteção contra *malware* ---------- 35
3.3.10.1 Implantar proteção contra malware 36
3.3.11 Controle 11: recuperação de dados ---------- 36
3.3.11.1 Estabelecer e manter um processo de backup 36
3.3.12 Controle 12: gerenciamento de infraestrutura de rede ---------- 37
3.3.12.1 Estabelecer e manter um inventário de estrutura de rede 37
3.3.12.2 Aplicar configuração segura em dispositivos de rede 37

3.3.13 Controle 14: conscientização e treinamento de segurança ---------- 37
3.3.13.1 Treinamento de conscientização de segurança 38
3.3.14 Controle 15: gerenciamento de fornecedores de serviços ---------- 38
3.3.14.1 Estabelecer e manter inventário de fornecedores 39
3.3.14.2 Avaliação de fornecedores de serviços 39
3.3.15 Controle 17: gerenciamento de resposta a incidentes ---------- 39
3.3.15.1 Estabelecer e manter um plano de resposta a incidentes 39
3.4 Priorização de implementação de controles 40
4 CONSIDERAÇÕES FINAIS 41
REFERÊNCIAS 43

INTRODUÇÃO

Embora o Brasil apresente os menores números de desemprego no período entre 2014 a 2024, segundo dados apontados pela PNAD (Pesquisa Nacional de Amostra de Domicílios) divulgada pelo IBGE (Instituto Brasileiro de Geografia e Estatística) em 31 de outubro de 2024, os números de micro e pequenas empresas atingiram números recordes no período histórico, com 3,3 milhões de novos pequenos negócios criados apenas entre Janeiro e Outubro de 2024, de acordo com levantamento realizado pelo SEBRAE (Serviço Brasileiro de Apoio às Micro e Pequenas Empresas). Isso aliado à contínua digitalização dos negócios e o estabelecimento de uma economia de dados, demonstram um cenário de risco em segurança da informação, uma vez que grande parte dessas micro e pequenas empresas não possuem a capacidade tanto financeira quanto de expertise para proteger seus dados e negócios.

Com o intuito de proteger tanto dados pessoais para estar em conformidade com as regulações, como por exemplo, a LGPD (Lei Geral de Proteção de Dados) quanto para garantir a plena continuidade dos negócios, evitando eventos que ameacem a confidencialidade, integridade e disponibilidade das informações empresariais, é mais do que nunca necessário o entendimento dos fundamentos de segurança da informação.

O trabalho é viável pela grande oferta de recursos tecnológicos e organizacionais disponíveis para aplicação no contexto de uma microempresa que atuam como controles de segurança da informação, tais como políticas de controle de acesso, softwares de gerenciamento de senhas, entre outros, assim como o crescente interesse geral pelo tema da segurança da informação, devido a significativa dependência de sistemas de informação na atividade econômica.

A partir disso, a importância do trabalho reside no mútuo interesse, tanto de organizações quanto dos proprietários dos dados processados em diferentes contextos, pelo aumento da capacidade de proteção de seus dados e informações.

O objetivo geral é levantar como organizações com pouca ou nenhuma medida de segurança da informação implementada podem melhorar seu cenário de proteção de dados com implementações simples.

Como objetivo específico, o trabalho pretende demonstrar o impacto da aplicação dos controles básicos de segurança da informação, no aumento do nível de maturidade de uma microempresa.

A hipótese central do trabalho é de que a aplicação de controles básicos de segurança da informação tem um impacto significativo no nível de maturidade. Com a rápida digitalização da economia no contexto brasileiro, muitas organizações não foram capazes de estabelecer um ambiente seguro para os dados e informações cruciais para a empresa, fazendo com que seus mais valiosos ativos de informação estejam em um ambiente de pouco ou nenhuma proteção, fazendo com que controles básicos de segurança da informação consigam impactar de maneira significativa no seu nível de maturidade em segurança.

O percurso metodológico deste trabalho é uma pesquisa exploratória com revisão bibliográfica sobre controles de segurança da informação e sua relevância no contexto organizacional, combinado com uma análise qualitativa/quantitativa de como tais controles podem influenciar no nível de maturidade de segurança da informação. O sujeito da pesquisa será uma microempresa do setor de comunicação. Os indicadores serão baseados na matriz de maturidade de segurança da informação definida pelo framework CIS *Controls*.

1 FUNDAMENTAÇÃO TEÓRICA

1.1 Controles de segurança da informação

Segundo Sêmola (2013), informações são a base da tomada de decisões para organizações dos mais variados segmentos e se tornam assim um valioso diferencial competitivo em relação aos negócios, dessa forma, é preciso que haja controle em relação às informações organizacionais.

São considerados controles de segurança da informação, ações que promovam mudanças aos riscos de segurança, podendo ser de natureza administrativa, técnica, gerencial ou legal, de forma que esses riscos possam ser gerenciados (Hintzbergen et al, 2018). Ainda conforme Sêmola (2013), controles de segurança da informação podem ser definidos em três categorias, sendo eles: controles preventivos, detectivos ou corretivos.

De acordo com a Norma Brasileira ABNT NBR ISO/IEC 27002, uma organização deve se basear em seus critérios de aceitação e tratamento de risco e nas legislações e regulamentações que está submetida, sejam essas nacionais ou não, para realizar a seleção dos controles de segurança da informação que serão implementados em sua estrutura.

Por fim, podemos usar a definição de Fernandes (2009), que resumiu controles de segurança da informação como elementos cruciais da regulação auto imposta pela gestão de uma organização.

1.2 Risco em segurança da informação

Fernandes (2009) define risco de segurança como um evento possível de acontecer que pode causar algum tipo de dano à organização. Hintzbergen et al (2018) acrescenta que o risco à segurança da informação está relacionado à capacidade de exploração de uma vulnerabilidade em um ativo de informação por um agente de ameaça e o dano que isso pode causar a organização.

Como exemplo, podemos imaginar uma organização que processa e armazena dados sensíveis de clientes, como informações financeiras. Uma vulnerabilidade, como falta de atualização de segurança no software utilizado para gerenciar esses dados representaria um risco.

Com o intuito de amenizar os possíveis danos causados, organizações implementam protocolos para entender a causa raiz de um risco e estabelecer a ele uma estimativa mensurável de probabilidade e impacto, como definido por Hintzbergen et al (2018) ao abordar o conceito de análise de risco.

A implementação de protocolos de análise de risco, como os definidos por Hintzbergen et al (2018), ajuda a transformar riscos em informações mensuráveis, que permitem que as organizações identifiquem e entendam os potenciais riscos que podem afetar o negócio, sendo de suma importância para proteger os ativos de informação.

1.3 Maturidade em segurança da informação

De acordo com o framework para governança e gestão da informação e tecnologia empresarial COBIT (2019), maturidade é uma maneira de alto nível de expressar a capacidade de uma empresa ou área atingir certos parâmetros definidos em seus processos de gestão de segurança da informação.

Dentro dos diferentes frameworks existentes para gestão de tecnologia da informação e governança existem diferentes critérios para medição do nível de maturidade em segurança da informação de uma empresa. O COBIT (2019) classifica a maturidade em seis níveis, sendo eles, incompleto, inicial, gerenciável, definido, quantitativo e otimizado, já o framework CIS *Controls* (2021) estabelece os níveis sendo não existente, inicial, repetitivo, definido, gerenciado e otimizado.

A importância de estabelecer um modelo de maturidade em segurança da informação em uma organização advém do fato desses modelos fornecerem uma estrutura para mensurar o desempenho atual de uma empresa em relação a práticas estabelecidas, permitindo identificar lacunas e oportunidades de melhoria, isso ajuda a direcionar esforços para o fortalecimento contínuo dos controles de segurança e a mitigação de riscos. Além disso, modelos de maturidade oferecem uma visão clara sobre o estágio de desenvolvimento de processos, possibilitando que as organizações estabeleçam planos de ação para alcançar níveis mais elevados de capacidade e eficácia.

Baseado no modelo de maturidade do COBIT (2019), uma organização que se encontra no nível "inicial" pode estar apenas começando a formalizar seus processos

de segurança, enquanto uma empresa no nível "otimizado" já possui práticas de segurança altamente eficientes e adaptáveis.

Modelos de maturidade são metodologias estruturadas utilizadas para avaliar e aprimorar o desenvolvimento e a eficiência de processos dentro de uma organização, sendo fundamentais no contexto da governança e gestão de tecnologia da informação. Ao fornecer uma abordagem escalonada e mensurável, esses modelos permitem que as empresas não só monitorem seu desempenho atual, mas também tracem um caminho claro para o aprimoramento contínuo.

1.4 Governança em segurança da informação

Segundo o IBGC (Instituto Brasileiro de Governança Corporativa), a governança corporativa tem como foco a geração de valor para todas as partes interessadas de uma corporação, utilizando-se de regras, estruturas e processos que orientam as ações dos agentes da organização na busca por atingir os objetivos das partes.

Baseado no conceito acima, podemos então compreender a governança de segurança da informação como uma série de processos que norteiam a utilização dos sistemas de informação de forma a minimizar seus riscos e atingir os objetivos das partes interessadas, como podemos notar em Ribeiro (2015), quando define o objetivo da governança de segurança da informação como a geração de métodos funcionais de gerenciamento que garantam o alinhamento entre os interesses dos envolvidos e a melhoria de resultados.

Devido a sua natureza processual e fortemente estruturada, durante os últimos anos diversos frameworks, normas, guias, códigos de boas práticas, entre outros, foram desenvolvidos para auxiliar na aplicação da governança de segurança da informação. Dessa forma, os próximos sub-capítulos visam uma apresentação de dois dos mais famosos frameworks utilizados hoje, o COBIT e o CIS *Controls*, além da principal norma associada a segurança da informação a Norma Brasileira ABNT NBR ISO/IEC 27002.

1.4.1 COBIT

De acordo a introdução da edição de 2019 do COBIT, ele é um framework para governança e gerenciamento de informação e tecnologia com objetivo de atingir todas as áreas de uma corporação.

O COBIT 2019 diferencia categoricamente governança de gerenciamento, definindo a governança como uma disciplina que garante a avalição das necessidades, condições e opções das partes envolvidas para a definição de objetivos corporativos balanceados, a priorização e tomada de decisão como norteador da direção da organização e o monitoramento da performance e conformidade da organização baseado em seus objetivos.

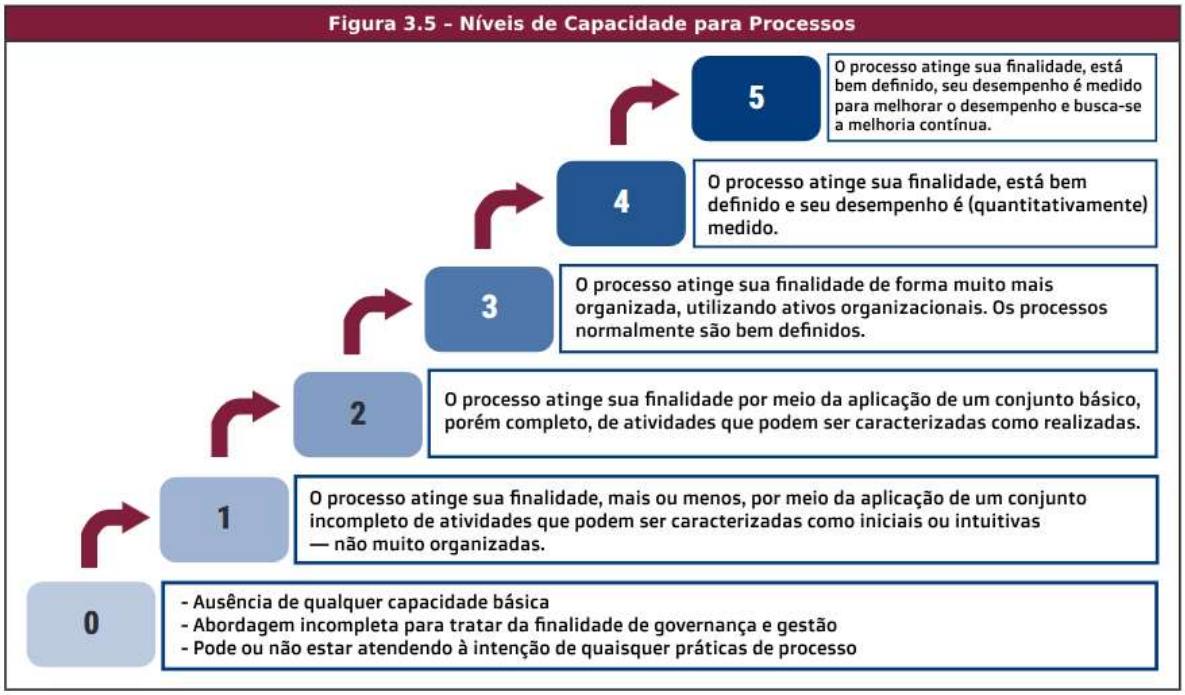
O COBIT define componentes como processos, estruturas organizacionais, políticas, procedimentos, cultura corporativa, informações e infraestrutura de serviços para alicerçar seu sistema de governança, e uma vez bem aplicados, esses componentes colaboram com a construção de sistema robusto de segurança da informação (ISACA,2019, p. 20).

O COBIT 2019 ainda fornece uma estrutura de mensuração de níveis de capacidade que podem ser utilizados para avaliar a maturidade de processos e controles relacionados à segurança da informação, como podemos ver na Figura 1. Com isso, é possível identificar pontos fracos, planejar melhorias e acompanhar a evolução da maturidade ao longo do tempo.

Para alcançar um nível elevado de maturidade em segurança da informação, é essencial implementar práticas recomendadas relacionadas aos processos descritos no framework. Por exemplo, o processo DSS05 *manage security services* é composto de práticas como identificação de ativos críticos, implementação de controle de acesso e tratamento de vulnerabilidades, isso explicita a interligação entre o framework COBIT e atividades práticas de segurança da informação (ISACA, 2019, p. 257-261).

Ao permitir a medição da maturidade com base em níveis de capacidade e ao oferecer orientações específicas para a implementação de processos de segurança, o framework se consolida como um dos mais relevantes no campo da governança de TI.

Figura 1 - Classificação de níveis de maturidade do framework COBIT.



Fonte: ISACA. COBIT® 2019 Framework: Introduction & Methodology. Schaumburg, 2019. 64p.

1.4.2 CIS *Controls*

Em sua introdução, o CIS *Controls* (2021) se define como uma comunidade internacional formada por indivíduos e instituições que visam compartilhar ideias sobre ciberataques de forma a compreender suas causas raiz e a partir disso desenvolver práticas de defesa.

Desde sua versão 8.1, o CIS *Controls* é dividido em três grupos de implementação de controles (*Controls Implementation Groups* IGs), cada um deles visando atender as necessidades de diferentes tipos de organizações, levando em consideração seu tamanho e expertise em segurança da informação. De forma resumida, o CIS *Controls* utiliza a seguinte divisão para categorizar os diferentes grupos de implementação:

IG1: Empresas de pequeno a médio porte com expertise em tecnologia da informação e cibersegurança limitada.

IG2: Empresas com pessoal dedicado à proteção e gerenciamento da infraestrutura de tecnologia da informação.

IG3: Empresas com pessoal dedicado e especializado em diferentes áreas de segurança da informação.

1.4.3 Mapeamento de controles do CIS Controls e da Norma Brasileira ABNT NBR ISO/IEC 27002

O CIS *Controls* v8, publicado pelo *Center for Internet Security* (CIS, 2021), estipula um conjunto de controles projetados para proteger sistemas e dados contra as principais ameaças de segurança da informação. Já a ISO/IEC 27001:2022, conforme detalhado na ISO/IEC 27002 (ISO, 2022), fornece uma estrutura para o estabelecimento, implementação, manutenção e melhoria de um Sistema de Gestão de Segurança da Informação (SGSI).

Embora diferentes em seus focos, existe grande sinergia entre os controles apresentados pelos CIS *Controls* v8 e pela ISO/IEC 27002. O controle 1 do CIS (inventário e controle de ativos empresariais), por exemplo, está diretamente relacionado com o controle 5.9 da ISO/IEC 27002, que aborda o inventário de ativos e a responsabilidade sobre eles. Ambos visam assegurar que todos os ativos de informação estejam devidamente identificados e gerenciados.

Outro exemplo de correlação ocorre entre o controle 4 do CIS (configuração segura de ativos empresariais e *software*) e os controles 8.9 (configuração de segurança) e 8.10 (gestão de vulnerabilidades técnicas) da ISO 27002, com o incentivo à adoção de configurações seguras e atualizadas como prática fundamental de segurança.

Adicionalmente, o controle 6 do CIS (gerenciamento de controle de acesso) corresponde aos controles da seção 5 da ISO/IEC 27002, especialmente o 5.15 (política de controle de acesso) e o 5.16 (gestão de acesso de usuários, enfatizando a importância da aplicação do princípio do menor privilégio, de autenticação forte e de gerenciamento de credenciais de acesso.

Outro ponto de convergência ocorre com o controle 17 do CIS (gerenciamento de resposta a incidentes), que se alinha aos controles da seção 5.24 a 5.26 da ISO/IEC 27002, tratando da gestão de eventos e incidentes de segurança da informação. Tanto o CIS quanto a ISO reforçam a necessidade de estabelecer processos para detecção, resposta e aprendizado contínuo a partir de incidentes.

Essa interseção entre as abordagens permite que organizações utilizem os CIS *Controls* como uma base prática e técnica para alcançar a conformidade com os requisitos normativos da ISO/IEC 27001, facilitando assim a implementação de um Sistema de Gestão de Segurança da Informação, uma vez que, de acordo com o

próprio *Center for Internet Security* (2021), os CIS *Controls* podem ser utilizados como um caminho inicial e operacional para atender aos requisitos de segurança da ISO/IEC 27002 para organizações que buscam diretrizes técnicas.

2 METODOLOGIA

Para investigar o impacto da implementação de controles básicos de segurança da informação no nível de maturidade de uma microempresa, adotou-se uma abordagem metodológica qualitativa, centrada em um estudo de caso. A pesquisa qualitativa permite compreender fenômenos complexos a partir de uma perspectiva interpretativa e contextualizada, sendo adequada para explorar as nuances envolvidas na adoção de práticas de segurança por organizações de pequeno porte (Creswell, 2014). A escolha por esse tipo de abordagem se justifica pela necessidade de aprofundamento na realidade específica da empresa estudada, buscando captar os desafios, percepções e resultados observados ao longo do processo de implementação dos controles.

O estudo de caso foi realizado em uma microempresa do setor de comunicação, com menos de dez colaboradores e uma estrutura de segurança da informação incipiente. A coleta de dados ocorreu por meio de entrevistas com os gestores e observação direta dos processos. O objetivo foi compreender como os controles básicos propostos pelo framework CIS *Controls*, especificamente dentro do grupo IG1, podem ser implantados e quais efeitos essas ações causariam na maturidade organizacional em segurança da informação.

Durante o estudo, foram priorizados controles considerados fundamentais, como a gestão de ativos, o controle de acessos, a aplicação de atualizações e a realização de backups regulares. Esses controles foram selecionados por sua viabilidade técnica e financeira, além de seu alto impacto em ambientes com infraestrutura limitada.

3 ESTUDO DE CASO

3.1 Apresentação da empresa

A empresa utilizada no presente estudo de caso é uma organização de porte pequeno do ramo da comunicação que produz planejamentos de campanha e conteúdo para marcas de diferentes segmentos.

Devido ao seu pequeno número de colaboradores, a empresa não possui profissionais designados para as áreas de tecnologia da informação e sua infraestrutura tecnológica é bastante enxuta, uma vez que a empresa não possui sede física, composta basicamente por um ambiente em nuvem para troca de informações.

Os principais dados processados pela empresa são listas de e-mails, valores de investimento em mídia, resultados das campanhas de comunicação e dados pessoais de fornecedores, parceiros e clientes.

Embora a empresa possua um sistema simples de classificação de informações que diferencia documentos internos e externos e um sistema de acesso a informações baseado em funções, não existe nenhum procedimento padrão relacionado à segurança da informação, como políticas. Um panorama geral da situação da organização quanto aos controles referentes ao grupo de implementação IG1 do CIS *Controls* é referenciado na Figura 2.

Figura 2 - Situação geral da organização quanto aos controles existentes no CIS Controls.

Cntroles CIS Controls V8		Quantidade de itens por nível de maturidade						Nível de Maturidade Médio	
		0 - Não Existente	1 - Inicial	2 - Repetitivo	3 - Definido	4 - Gerenciado	5 - Otimizado		
1	Inventário e controle de ativos da empresa	0	1	0	0	0	0	1,00	1 - Inicial
2	Inventário e controle de ativos de software	1	0	0	0	0	0	0,00	0 - Não Existente
3	Proteção de dados	0	1	0	0	0	0	1,00	1 - Inicial
4	Configuração segura de ativos corporativos e software	1	0	0	0	0	0	0,00	0 - Não Existente
5	Gestão de Contas	0	1	0	0	0	0	1,00	1 - Inicial
6	Gerenciamento de controle de acesso	0	1	0	0	0	0	1,00	1 - Inicial
7	Gerenciamento Contínuo de Vulnerabilidade	1	0	0	0	0	0	0,00	0 - Não Existente
8	Gerenciamento de registro de auditoria	1	0	0	0	0	0	0,00	0 - Não Existente
9	Proteções de e-mail e navegador da web	0	1	0	0	0	0	1,00	1 - Inicial
10	Defesas contra malware	0	1	0	0	0	0	1,00	1 - Inicial
11	Recuperação de dados	0	1	0	0	0	0	1,00	1 - Inicial
12	Gerenciamento de infraestrutura de rede	1	0	0	0	0	0	0,00	0 - Não Existente
14	Conscientização de segurança e treinamento de habilidades	1	0	0	0	0	0	0,00	0 - Não Existente
15	Gestão de Provedores de Serviços	1	0	0	0	0	0	0,00	0 - Não Existente
17	Gerenciamento de resposta a incidentes	1	0	0	0	0	0	0,00	0 - Não Existente
Índice Geral de Maturidade		**8**	**7**	**0**	**0**	**0**	**0**	**1,00**	**1 - Inicial**

Fonte: Elaborado pelo autor.

3.2 Grupo de implementação

Baseado no escopo empresarial em que a organização objeto do estudo de caso se encontra, foi escolhido o grupo de implementação IG1 do CIS *Controls* versão 8.

O grupo de implementação IG1 é composto por 15 controles e, de acordo com o CIS *Controls* (2021), suas salvaguardas foram desenvolvidas para ambientes organizacionais com expertise limitada em segurança da informação, visando ataques e vulnerabilidades generalistas, e para atuar em conjunto com software e hardware comerciais de pequeno porte.

3.3 Controles e salvaguardas

3.3.1 Controle 1: inventário e controle de ativos empresariais

É necessário que a organização tenha conhecimento sólido dos ativos que possui. Um inventário bem elaborado permite a gestão adequada dos ativos empresariais, permitindo a identificação e proteção de ativos críticos, além de colaborar com o monitoramento de atividades suspeitas nesses ativos.

A Figura 3 demonstra o número do controle, título, descrição, grupo de implementação e nível de maturidade da organização nesse controle antes das medidas propostas.

Figura 3 - Nível de maturidade do controle 1 da organização antes das medidas propostas pelo estudo de caso.

Controle CIS	Título	Descrição	IG1	IG2	IG3	Maturidade
1	Inventário e controle de ativos da empresa	*Gerenciar ativamente (inventariar, rastrear e corrigir) todos os ativos da empresa (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não informáticos / IoT - Internet das Coisas; e servidores) conectados à infraestrutura fisicamente, virtualmente, remotamente, e aqueles em ambientes de nuvem, para saber com precisão a totalidade de ativos que precisam ser monitorados e protegidos dentro da empresa. Isso também apoiará a identificação de ativos não autorizados e não gerenciados para remover ou corrigir.*	x			1 - Inicial

Fonte: Elaborado pelo autor.

3.3.1.1 Estabelecer e manter inventário detalhado de ativos empresariais

Deverá ser criada uma planilha que contenha dados referentes a todos os ativos empresariais, como nome do colaborador responsável, tipo de dispositivo,

sistema operacional, endereço de IP caso o dispositivo utilize endereço fixo, endereço MAC e se o dispositivo se encontra em uso ou não.

Esse inventário deverá ser revisado periodicamente, com intuito de mantê-lo atualizado. Devido à baixa rotatividade de dispositivos acessando o ambiente da empresa, fica definido que a revisão deverá ocorrer a cada 12 meses.

3.3.1.2 Endereçar ativos não autorizados

Sempre que um novo dispositivo tentando acessar o ambiente da organização for identificado, uma verificação manual deverá ser feita para analisar se este dispositivo deve ou não ter seu acesso permitido.

3.3.2 Controle 2: inventário e controle de ativos de *software*

A organização deverá ter conhecimento de quais softwares e suas respectivas versões são utilizados em seu ambiente. Isso permite que a empresa possa mitigar vulnerabilidades de software conhecidas e evitar uso de softwares não seguros.

A Figura 4 demonstra o número do controle, título, descrição, grupo de implementação e nível de maturidade da organização nesse controle antes das medidas propostas.

Figura 4 - Nível de maturidade do controle 2 da organização antes das medidas propostas pelo estudo de caso.

Controle CIS	Título	Descrição	IG1	IG2	IG3	Maturidade
2	Inventário e controle de ativos de software	*Gerenciar ativamente (inventarie, rastreie e corrija) todos os softwares (sistemas operacionais e aplicações) na rede para que apenas softwares autorizados sejam instalados e possam ser executados, e que softwares não autorizados e não gerenciados sejam encontrados e impedidos de instalação ou execução.*	x			0 - Não Existente

Fonte: Elaborado pelo autor.

3.3.2.1 Estabelecer e manter um inventário de *software*

Deverão ser documentados todos os softwares autorizados para uso dentro do ambiente organizacional. O inventário deve conter o nome do software, a empresa fornecedora, data de instalação e qual a sua finalidade.

3.3.2.2 Garantir que o *software* autorizado receba suporte

A empresa deverá realizar uma revisão periódica do inventário de software com intuito de identificar se os softwares autorizados ainda recebem suporte técnico de seus fornecedores. Devido à extensa oferta de softwares e versões, essa revisão deverá ocorrer a cada 6 meses.

3.3.2.3 Endereçar *software* não autorizado

Sempre que identificado o uso de software não autorizado ou inseguro, a empresa deve garantir que o software seja removido dos dispositivos empresariais ou elaborar uma documentação expressa de exceção. Em casos em que uma exceção foi documentada, uma revisão mensal da autorização desse software deverá ser feita.

3.3.3 Controle 3: proteção de dados

Devido a crescente digitalização, ainda mais considerando empresas que não possuem infraestrutura física, a superfície do tráfego e aceso a dados empresariais aumentou exponencialmente. A sistematização da proteção de dados ajuda a evitar que dados sensíveis sejam perdidos, assim como auxilia na conformidade com regulamentações de proteção de dados pessoais.

A Figura 5 demonstra o número do controle, título, descrição, grupo de implementação e nível de maturidade da organização nesse controle antes das medidas propostas.

Figura 5 - Nível de maturidade do controle 3 da organização antes das medidas propostas pelo estudo de caso.

Controle CIS	Título	Descrição	IG1	IG2	IG3	Maturidade
3	Proteção de dados	*Desenvolver processos e controles técnicos para identificar, classificar, manusear, reter e descartar dados com segurança.*	x			1 - Inicial

Fonte: Elaborado pelo autor.

3.3.3.1 Estabelecer e manter um processo de gerenciamento de dados

Um documento estabelecendo regras de acesso à dados será criado estabelecendo quem pode acessar quais dados, como serão armazenados, por quanto tempo serão retidos e como descartá-los. Dessa forma, a organização terá uma visão clara de qual é o ciclo de vida dos dados que processa.

3.3.3.2 Estabelecer e manter um inventário de dados

Todos os dados processados pela empresa deverão ser inventariados em uma planilha estipulando quem tem acesso a esse dado, seu local de armazenamento, seu período de retenção e sua correta classificação entre público (externos), internos e confidenciais.

3.3.3.3 Configurar listas de controles de acesso a dados

O ambiente de nuvem da organização deverá ser configurado para que dados sejam acessados apenas por pessoas autorizadas e com uma finalidade definida. O princípio da “necessidade de saber”, onde o acesso só é instituído a dados necessários para que determinado colaborador execute suas funções organizacionais, deverá ser aplicado.

Os acessos deverão ser permitidos sob análise e revogados assim que não tenham mais necessidade de serem acessados. As listas de acesso deverão ser revisadas de maneira periódica a cada 12 meses para garantir sua adequação.

3.3.3.4 Aplicar retenção de dados

Prazos para armazenamento dos dados serão definidos e deverão obrigatoriamente ser descartados após o fim do tempo de retenção.

3.3.3.5 Descartar dados de forma segura

Os dados deverão ser excluídos do ambiente de nuvem da organização de forma definitiva, e antes da exclusão todos os compartilhamentos realizados desses dados deverão ser removidos.

3.3.3.6 Criptografar dados em dispositivos de usuários

As ferramentas *BitLocker* (*Windows*) e *FileVault* (*MacOS*) serão ativados nos dispositivos da organização para proteger dados armazenados localmente.

3.3.4 Controle 4: configuração segura de ativos de *software* empresariais

Padrões de configuração que sejam gerenciáveis dão controle à organização de como seus ativos e *softwares* são utilizados. Fornecedores de sistemas computacionais focam na facilidade de uso na configuração básica de seus produtos, o que pode criar brechas de segurança. Sistematizar a configuração garante à organização rastreabilidade de mudanças em seus ativos e sua correta usabilidade.

A Figura 6 demonstra o número do controle, título, descrição, grupo de implementação e nível de maturidade da organização nesse controle antes das medidas propostas.

Figura 6 - Nível de maturidade do controle 4 da organização antes das medidas propostas pelo estudo de caso.

Controle CIS	Título	Descrição	IG1	IG2	IG3	Maturidade
4	Configuração segura de ativos corporativos e software	*Estabelecer e manter a configuração segura de ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não informáticos / IoT; e servidores) e software (sistemas operacionais e aplicativos).*	x			0 - Não Existente

Fonte: Elaborado pelo autor.

3.3.4.1 Estabelecer e manter um processo de configuração segura

Uma lista com padrões mínimos para configurações de dispositivos será criada, estabelecendo período para aplicação de atualizações automáticas de *software* e sistemas operacionais, obrigatoriedade da ativação de firewall e padrões de senha forte.

3.3.4.2 Estabelecer e manter configuração segura da infraestrutura de rede

Como a empresa não possui estrutura física de rede, uma vez que todos os colaboradores atuam de maneira remota em um ambiente de nuvem, fica estabelecido que apenas conexões privadas e confiáveis devem ser utilizadas para acesso ao ambiente organizacional.

3.3.4.3 Configurar bloqueio automático de sessão

Todos os dispositivos utilizados para atividades organizacionais devem ser configurados para entrar em modo de bloqueio após 5 minutos de inatividade.

3.3.4.4 Implementar e gerenciar *firewall* em servidores

Os serviços de nuvem utilizados como ambientes organizacionais têm seus sistemas de *firewall* configurados e ativos durante todo o tempo.

3.3.4.5 Implementar firewall em dispositivos de usuário final

Todos os dispositivos utilizados para atividades organizacionais, sendo o sistema operacional *Windows* ou *macOS* terão habilitados os serviços de *firewall* padrão dos sistemas operacionais como medida mínima de proteção.

3.3.4.6 Gerenciar de forma segura ativos e *software* da empresa

É permitido o uso apenas de protocolos que garantam conexão segura, como por exemplo, SSH e HTTPS.

3.3.5 Controle 5: gerenciamento de contas

A gestão criteriosa de identidades e credenciais constitui componente indispensável da segurança da informação, dado que agentes mal-intencionados tendem a explorar acessos legítimos em vez de recorrer a técnicas avançadas de

invasão. O risco eleva-se em contas privilegiadas, que facultam a criação de novos usuários ou a alteração de configurações críticas, e em contas de serviço, frequentemente desconhecidas ou partilhadas por equipes externas, ampliando a superfície de ataque.

A Figura 7 demonstra o número do controle, título, descrição, grupo de implementação e nível de maturidade da organização nesse controle antes das medidas propostas.

Figura 7 - Nível de maturidade do controle 5 da organização antes das medidas propostas pelo estudo de caso.

Controle CIS	Título	Descrição	IG1	IG2	IG3	Maturidade
5	Gestão de Contas	*Usar processos e ferramentas para atribuir e gerenciar autorização para credenciais para contas de usuário, incluindo contas de administrador, bem como contas de serviço, para ativos corporativos e software.*	x			1 - Inicial

Fonte: Elaborado pelo autor.

3.3.5.1 Estabelecer e manter inventário de contas

Uma lista atualizada de todos os usuários com acesso ao ambiente organizacional será mantida. Dessa forma a empresa mantém controle de quais contas são permitidas em seu ambiente, facilitando a identificação de acessos indevidos.

3.3.5.2 Utilizar senhas únicas

A utilização de senhas únicas para acesso aos diferentes sistemas organizacionais deverá ser requisito mandatório e constantemente reforçado pela direção da organização. Além disso, o uso de gerenciadores de senha, como o *Bitwarden*, deve ser recomendado sempre quando for pertinente.

3.3.5.3 Desativar contas inativas

Quando um colaborador tiver sua relação com a empresa encerrada, sua conta, juntamente de seus respectivos acessos deverão ser desativados. O mesmo processo é válido para contas inativas há 30 dias corridos completos.

3.3.5.4 Restringir privilégio de administrador a contas dedicadas

A segregação entre usuário padrão e administrativo é obrigatória. Contas separadas serão criadas para diferenciar o usuário utilizado para tarefas diárias da empresa e para usuário utilizado para configurações administrativas do ambiente organizacional.

3.3.6 Controle 6: gerenciamento de controle de acesso

Aplicar de forma consistente o princípio do menor privilégio é decisivo para limitar a superfície de ataque e reduzir o impacto de credenciais comprometidas. Ao garantir que cada usuário possua apenas os direitos estritamente necessários, a organização minimiza o acesso indevido a dados sensíveis. O uso obrigatório da autenticação multi fator (AMF) em aplicações expostas à internet e acessos remotos previne a exploração de senhas fracas, vazadas ou reutilizadas.

A Figura 8 demonstra o número do controle, título, descrição, grupo de implementação e nível de maturidade da organização nesse controle antes das medidas propostas.

Figura 8 - Nível de maturidade do controle 6 da organização antes das medidas propostas pelo estudo de caso.

Controle CIS	Título	Descrição	IG1	IG2	IG3	Maturidade
6	Gerenciamento de controle de acesso	*Usar processos e ferramentas para criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas de usuário, administrador e serviço para ativos e software corporativos.*	x			1 - Inicial

Fonte: Elaborado pelo autor

3.3.6.1 Estabelecer processo de concessão de acessos

Todo colaborador receberá, mediante solicitação formal via e-mail, somente as permissões mínimas necessárias ao desempenho de suas funções, reforçando o princípio da “necessidade de saber” e registrando a aprovação no sistema de gestão de identidades.

3.3.6.2 Estabelecer processo de revogação de acessos

No desligamento do colaborador ou mudança de função, todos os acessos serão revogados imediatamente conforme procedimento documentado, garantindo que nenhuma credencial ativa permaneça sem propósito.

3.3.6.3 Exigir AMF para aplicações expostas externamente

É obrigatória a autenticação multi fator em plataformas corporativas acessíveis via internet, reduzindo o risco de comprometimento por força-bruta ou vazamentos de senha.

3.3.6.4 Exigir AMF para acesso remoto ao ambiente corporativo

Como a infraestrutura organizacional se encontra em nuvem, qualquer conexão remota aos sistemas corporativos deve utilizar autenticação multi fator, para resguardar o ambiente contra ataques de *phishing* e similares.

3.3.6.5 Exigir AMF para acesso administrativo

Contas privilegiadas, como painéis de administração de serviços e consoles de gestão, devem estar configuradas obrigatoriamente com autenticação multi fator, evitando que invasores obtenham controle total do ambiente caso consigam a senha.

3.3.7 Controle 7: gerenciamento contínuo de vulnerabilidades

Manter um processo ativo de identificação e correção de falhas é imprescindível para reduzir a janela de exposição a ameaças conhecidas. A detecção antecipada de vulnerabilidades em sistemas operacionais, aplicativos e serviços, aliada à aplicação rápida de correções, impede que agentes mal-intencionados explorem brechas documentadas e eleva o nível geral de resiliência do ambiente corporativo.

A Figura 9 demonstra o número do controle, título, descrição, grupo de implementação e nível de maturidade da organização nesse controle antes das medidas propostas.

Figura 9 - Nível de maturidade do controle 7 da organização antes das medidas propostas pelo estudo de caso.

Controle CIS	Título	Descrição	IG1	IG2	IG3	Maturidade
7	Gerenciamento Contínuo de Vulnerabilidade	*Desenvolver um plano para avaliar e rastrear vulnerabilidades continuamente em todos os ativos corporativos dentro da infraestrutura da empresa, a fim de remediar e minimizar a janela de oportunidade para os invasores. Monitorar fontes da indústria pública e privada para novas informacões sobre ameacas e vulnerabilidades.*	x			0 - Não Existente

Fonte: Elaborado pelo autor

3.3.7.1 Estabelecer e manter um processo de gerenciamento de vulnerabilidades

Todos sistemas operacionais e aplicativos organizacionais tiveram sistema de atualização automática habilitados. Revisar semanalmente boletins de segurança e atualizações classificadas como críticas, assegurando que sejam aplicadas assim que identificadas.

3.3.7.2 Remediar vulnerabilidades

Quando identificado erro de segurança grave, por exemplo, falha de severidade crítica divulgada em um identificador CVE, impor atualização ou migração imediata do *software* afetado, documentando a ação e verificando a eficácia da correção.

3.3.8 Controle 8: gerenciamento de logs de auditoria

Registros de auditoria adequadamente configurados e analisados são fundamentais para detectar atividades suspeitas, reconstruir a cronologia de um incidente e demonstrar conformidade regulatória. A geração contínua e a revisão criteriosa desses registros permitem identificar acessos não autorizados, falhas operacionais e tentativas de violação.

A Figura 10 demonstra o número do controle, título, descrição, grupo de implementação e nível de maturidade da organização nesse controle antes das medidas propostas.

Figura 10 - Nível de maturidade do controle 8 da organização antes das medidas propostas pelo estudo de caso

Controle CIS	Título	Descrição	IG1	IG2	IG3	Maturidade
8	Gerenciamento de registro de auditoria	*Coletar, alertar, analisar e reter logs de auditoria de eventos que podem ajudar a detectar, compreender ou recuperar-se de um ataque.*	x			0 - Não Existente

Fonte: Elaborado pelo autor

3.3.8.1 Ativar e configurar *logs* de auditoria

A coleta de registros de acesso e eventos em todas as plataformas em nuvem e serviços corporativos foram habilitadas, definindo nível de detalhamento compatível com requisitos de segurança e privacidade, além de retenção em local protegido contra alterações não autorizadas.

3.3.8.2 Revisar logs de auditoria

Serão analisados registros sempre que houver incidentes ou indícios de comportamento anômalo, correlacionando eventos relevantes, produzindo relatórios de investigação e documentando lições aprendidas para aprimorar controles existentes.

3.3.9 Controle 9: proteção de *e-mail* e navegador *web*

E-mail e navegação são vetores preferenciais para tentativas de *phishing* e distribuição de *malware*. A adoção de mecanismos de validação de remetente e a configuração segura dos navegadores reduzem significativamente a probabilidade de entrega de mensagens fraudulentas, execução de códigos maliciosos e instalação indevida de arquivos contaminados.

A Figura 11 demonstra o número do controle, título, descrição, grupo de implementação e nível de maturidade da organização nesse controle antes das medidas propostas.

Figura 11 - Nível de maturidade do controle 9 da organização antes das medidas propostas pelo estudo de caso.

Controle CIS	Título	Descrição	IG1	IG2	IG3	Maturidade
9	*Proteções de e-mail e navegador da web*	*Melhorar as proteções e detecções de ameaças de vetores de e-mail e web, pois essas são oportunidades para os invasores manipularem o comportamento humano por meio do engajamento direto.*	x			1 - Inicial

Fonte: Elaborado pelo autor

3.3.9.1 Configurar proteção de *e-mail*

Serão implementados nos domínios corporativos os registros SPF (*Sender Policy Framework*), DKIM (*DomainKeys Identified Mail*) e DMARC (*Domain-based Message Authentication, Reporting and Conformance*), garantindo a autenticação de remetentes, a integridade das mensagens e relatórios de falhas de entrega ou tentativas de falsificação.

3.3.9.2 Configurar proteção de navegadores

Serão padronizados o uso de navegadores reconhecidos por atualizações de segurança rápidas, ativando bloqueio de janelas *pop-up*, impedindo *downloads* automáticos e aplicando listas de bloqueio de sites maliciosos.

3.3.10 Controle 10: proteção contra *malware*

A presença constante de código malicioso — vírus, *ransomware*, *spyware* e *trojans* — torna indispensável a adoção de mecanismos automáticos de prevenção, detecção e resposta. Uma solução antivírus confiável com proteção em tempo real diminui drasticamente o risco de execução de arquivos infectados.

A Figura 12 demonstra o número do controle, título, descrição, grupo de implementação e nível de maturidade da organização nesse controle antes das medidas propostas.

Figura 12 - Nível de maturidade do controle 10 da organização antes das medidas propostas pelo estudo de caso.

Controle CIS	Título	Descrição	IG1	IG2	IG3	Maturidade
10	Defesas contra malware	*Impedir ou controlar a instalação, disseminação e execução de aplicativos, códigos ou scripts maliciosos em ativos corporativos.*	x			1 - Inicial

Fonte: Elaborado pelo autor

3.3.10.1 Implantar proteção contra *malware*

Serão instalados em todos os dispositivos corporativos software antivírus, mantendo a varredura em tempo real habilitada, atualizando assinaturas e mecanismos de detecção automaticamente e impedindo a desativação não autorizada do recurso por meio de políticas de administração.

3.3.11 Controle 11: recuperação de dados

Serão instalados em todos os dispositivos corporativos software antivírus, mantendo a varredura em tempo real habilitada, atualizando assinaturas e mecanismos de detecção automaticamente e impedindo a desativação não autorizada do recurso por meio de políticas de administração.

A Figura 13 demonstra o número do controle, título, descrição, grupo de implementação e nível de maturidade da organização nesse controle antes das medidas propostas.

Figura 13 - Nível de maturidade do controle 11 da organização antes das medidas propostas pelo estudo de caso.

Controle CIS	Título	Descrição	IG1	IG2	IG3	Maturidade
11	Recuperação de dados	*Estabelecer e manter práticas de recuperação de dados suficientes para restaurar ativos corporativos dentro do escopo para um estado pré-incidente e confiável.*	x			1 - Inicial

Fonte: Elaborado pelo autor.

3.3.11.1 Estabelecer e manter um processo de *backup*

As opções de backup automático da infraestrutura de nuvem utilizada pela organização serão ativadas para garantir que todos os arquivos sejam sincronizados continuamente. Um responsável será definido para realizar verificações semanais da conclusão dos *backups*, analisando o histórico de versões e o status de sincronização para assegurar a integridade dos arquivos.

Além disso, uma cópia mensal desses arquivos será mantida em uma mídia externa (HD criptografado) guardada fora do ambiente principal da organização.

3.3.12 Controle 12: gerenciamento de infraestrutura de rede

Apesar da ausência de uma rede local tradicional, a infraestrutura mínima de rede usada pelos colaboradores remotos da empresa exige atenção quanto à segurança dos dispositivos que provêm conectividade à internet.

A Figura 14 demonstra o número do controle, título, descrição, grupo de implementação e nível de maturidade da organização nesse controle antes das medidas propostas.

Figura 14 - Nível de maturidade do controle 12 da organização antes das medidas propostas pelo estudo de caso.

Controle CIS	Título	Descrição	IG1	IG2	IG3	Maturidade
12	Gerenciamento de infraestrutura de rede	*Estabelecer, implementar e gerenciar ativamente (rastrear, reportar, corrigir) dispositivos de rede, a fim de evitar que invasores explorem serviços de rede e pontos de acesso vulneráveis.*	x			0 - Não Existente

Fonte: Elaborado pelo autor

3.3.12.1 Estabelecer e manter um inventário de estrutura de rede

Será realizado um levantamento dos dispositivos de rede utilizados pelos colaboradores remotos. Nesse inventário deverão constar, nome do colaborador, modelo do roteador, provedor de internet e a data da última revisão realizada.

A cada seis meses, os colaboradores serão instruídos a revisar as configurações do roteador e informar qualquer mudança realizada.

3.3.12.2 Aplicar configuração segura em dispositivos de rede

Todos os colaboradores serão orientados a alterar as senhas padrão de fábrica de seus respectivos roteadores e a utilizar senhas fortes.

3.3.13 Controle 14: conscientização e treinamento de segurança

A conscientização dos colaboradores é essencial para garantir que boas práticas sejam adotadas no dia a dia. Em uma microempresa com poucos integrantes, treinamentos ágeis e diretos mostram-se eficazes.

A Figura 15 demonstra o número do controle, título, descrição, grupo de implementação e nível de maturidade da organização nesse controle antes das medidas propostas.

Figura 15 - Nível de maturidade do controle 14 da organização antes das medidas propostas pelo estudo de caso.

Controle CIS	Título	Descrição	IG1	IG2	IG3	Maturidade
14	*Conscientização de segurança e treinamento de habilidades*	*Estabelecer e manter um programa de conscientização de segurança para influenciar o comportamento da força de trabalho a fim de se conscientizar sobre a segurança e se qualificar adequadamente para reduzir os riscos de segurança cibernética para a empresa.*	x			0 - Não Existente

Fonte: Elaborado pelo autor

3.3.13.1 Treinamento de conscientização de segurança

Com periodicidade trimestral, treinamentos de conscientização em segurança da informação serão providos aos colaboradores. Os treinamentos serão em formatos de e-mails, vídeos e reuniões online, abordando tópicos relevantes para segurança da informação da organização, como reconhecimento de *phishing*, uso de senhas fortes, importâncias de atualizações e boas práticas no compartilhamento de informações.

3.3.14 Controle 15: gerenciamento de fornecedores de serviços

Ter visibilidade e controle sobre os prestadores que processam dados empresariais é essencial para avaliar riscos e garantir conformidade com boas práticas e legislações como a LGPD.

A Figura 16 demonstra o número do controle, título, descrição, grupo de implementação e nível de maturidade da organização nesse controle antes das medidas propostas.

Figura 16 - Nível de maturidade do controle 15 da organização antes das medidas propostas pelo estudo de caso.

Controle CIS	Título	Descrição	IG1	IG2	IG3	Maturidade
15	Gestão de Provedores de Serviços	*Desenvolver um processo para avaliar os provedores de serviços que mantêm dados confidenciais, ou são responsáveis por plataformas ou processos de TI críticos de uma empresa, para garantir que esses provedores estejam protegendo essas plataformas e dados de forma adequada.*	x			0 - Não Existente

Fonte: Elaborado pelo autor

3.3.14.1 Estabelecer e manter inventário de fornecedores

Será criada uma planilha contendo informações relevantes sobre os fornecedores de serviço contratados pela organização. O inventário contará com nome do fornecedor, tipo de serviço prestado, dados acessados ou processados, link da política de privacidade e contato do suporte técnico.

3.3.14.2 Avaliação de fornecedores de serviços

Antes da contratação ou renovação de serviços, uma avaliação de critérios técnicos deverá ser realizada sobre a empresa prestadora do serviço. Histórico de incidentes de segurança, presença de controles de segurança e se a empresa possui certificações de segurança, como a ISO/IEC 27001 serão os critérios avaliados.

3.3.15 Controle 17: gerenciamento de resposta a incidentes

Responder rapidamente a incidentes é decisivo para minimizar impactos e manter a confiança de clientes e parceiros.

A Figura 17 demonstra o número do controle, título, descrição, grupo de implementação e nível de maturidade da organização nesse controle antes das medidas propostas.

Figura 17 - Nível de maturidade do controle 17 da organização antes das medidas propostas pelo estudo de caso.

Controle CIS	Título	Descrição	IG1	IG2	IG3	Maturidade
17	Gerenciamento de resposta a incidentes	Estabelecer um programa para desenvolver e manter uma capacidade de resposta a incidentes (por exemplo, políticas, planos, procedimentos, funções definidas, treinamento e comunicações) para preparar, detectar e responder rapidamente a um ataque.	x			0 - Não Existente

Fonte: Elaborado pelo autor.

3.3.15.1 Estabelecer e manter um plano de resposta a incidentes

Um colaborador será designado como responsável por registrar os detalhes referentes a incidentes de segurança da informação. Esse registro deverá ser feito em planilha específica para esse fim, contendo data em que o incidente foi descoberto, impacto, ação tomada e lições aprendidas.

Além disso, o contato de um fornecedor de serviço de segurança da informação externo deverá estar sempre disponível para suportar nas ações a serem tomadas

3.4 Priorização de implementação de controles

Devido a seu caráter fundamental na implementação de um sistema de gestão de segurança da informação, devido à necessidade de conhecer o que deve ser protegido dentro da organização, no primeiro momento serão priorizadas a implementação dos controles que identificam os ativos e sua criticidade e determinam as condições para acessá-los. Dessa forma, o foco estará nos controles inventário de ativos empresariais, inventário de software, configuração segura de ativos e software, gerenciamento de contas e controle de acesso – controles 1, 2, 4, 5 e 6, respectivamente.

No segundo momento da implementação, os controles com impacto técnico na gestão da segurança da informação que suportam a organização a lidar com eventuais problemas factuais de segurança e manter a continuidade de negócio serão priorizados. Esse segundo grupo de controles é composto por recuperação de dados, gerenciamento de vulnerabilidades, proteção de dados, proteção contra *malware*, proteção de *e-mail* e navegador – controles 11, 7, 3, 10 e 9, respectivamente.

Por fim, controles de implementação contínua, como os relacionados à cultura organizacional e que dependem da implementação dos controles supracitados para seu melhor aproveitamento. Sendo assim, os controles conscientização e treinamento de segurança (controle 14), gerenciamento de logs de auditoria (controle 8), gerenciamento de infraestrutura de rede (controle 12), gerenciamento de fornecedores (controle 15) e resposta a incidentes (controle 17).

4 CONSIDERAÇÕES FINAIS

O presente trabalho teve como objetivo investigar o impacto da aplicação de controles básicos de segurança da informação no nível de maturidade de uma microempresa brasileira, à luz do atual cenário de constante aceleração digital e do aumento significativo de novos pequenos negócios no Brasil, no contexto das exigências legais propostas pela LGPD. Utilizando como referência controles existentes no framework CIS *Controls*, o estudo buscou evidenciar como medidas tecnicamente simples podem elevar a segurança de um ambiente organizacional com recursos limitados.

A pesquisa foi conduzida por meio de um estudo de caso aplicado em uma microempresa do setor de comunicação com estrutura tecnológica enxuta e sem estruturação de controles de segurança da informação. A hipótese central do trabalho – “a aplicação de controles básicos de segurança da informação tem um impacto significativo no nível de maturidade” - foi confirmada, uma vez que as medidas propostas para aplicação representam ganho concreto no nível de maturidade em segurança da informação.

O objetivo geral de demonstrar como organizações com pouca ou nenhuma medida de segurança podem melhorar seu cenário de proteção de dados com medidas simples foi atingido com a documentação do processo de implementação dos 15 controles presentes no grupo de implementação IG1 do CIS *Controls* e suas respectivas salvaguardas.

O objetivo específico também foi alcançado ao ilustrar o impacto que os controles supracitados têm sobre o nível de maturidade geral de segurança da informação da empresa objeto do estudo de caso.

Em conclusão, o estudo revela que é possível que microempresas, inclusive de outros setores econômicos, aprimorem a forma como fazem a gestão da segurança da informação com ações de baixo investimento e pouca complexidade técnica.

Entre os principais aprendizados adquiridos no desenvolvimento do trabalho, podemos destacar o fato de que uma grande parcela dos riscos de segurança da informação, que podem afetar organizações dos mais variados tamanhos, pode ser mitigada com ações simples e de baixo custo, uma vez que sejam sistematizadas, revisadas e monitoradas.

Como proposta para trabalhos futuros, sugere-se a aplicação do mesmo modelo em organizações de outros portes e setores econômicos, com intuito de observar se os resultados apresentados são similares.

REFERÊNCIAS

ABREU, Carlos. Pequenos negócios somam 96% de todas as novas empresas criadas no Brasil. **Agência SEBRAE**, 22 out. 2024. Dados. Disponível em: https://agenciasebrae.com.br/dados/pequenos-negocios-somam-96-de-todas-as-novas-empresas-criadas-no-brasil/. Acesso em: 2 nov. 2024, às 19h52.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:** Tecnologia da informação — Técnicas de segurança — Código de prática para controles. Rio de Janeiro, 2013. 99p.

CENTER FOR INTERNET SECURITY. **CIS Controls:** v8. Nova Iorque, 2021, 87p.

CRESWELL, J. W. (2014). **Research Design: Qualitative, Quantitative, and Mixed Methods Approaches** (4th ed.). SAGE Publications.

FERREIRA, João Paulo da Silva. **Segurança da Informação nas Pequenas Empresas**. 2009. 36f. TG (Trabalho de Graduação do Curso Superior de Sistemas de Informação) Faculdade Anhanguera de Negócios e Tecnologias da Informação, Brasília, 2009.

HINTZBERGEN, Jule, et al. **Fundamentos de Segurança da Informação:** com base na ISO 27001 e na ISO 27002. Trad. Alan de Sá. 3ª ed. Rio de Janeiro : Brasport, 2018. 256p. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=1CVFDwAAQBAJ&oi=fnd&pg=PA1&dq=controles+de+seguran%C3%A7a+da+informa%C3%A7%C3%A3o&ots=YkAkWZmmBX&sig=r5-8z664JydnPZxkWGfj2xoavwI&redir_esc=y#v=onepage&q=controles%20de%20seguran%C3%A7a%20da%20informa%C3%A7. Acesso em: 5 nov. 2024, às 19h11.

ISACA. **COBIT® 2019 Framework:** Introduction & Methodology. Schaumburg, 2019. 64p.

NUNES, Julia. Desemprego cai a 6,4% no trimestre terminado em setembro, diz IBGE. **g1**, 30 out. 2024. Economia. Disponível em: https://g1.globo.com/economia/noticia/2024/10/31/desemprego-cai-a-64percent-no-trimestre-terminado-em-setembro-diz-ibge.ghtml. Acesso em: 2 nov. 2024, às 19h38.

SÊMOLA, Marcos. Gestão da Segurança da Informação: uma visão executiva. 2ª ed. Rio de Janeiro : Elsevier (Campus), 2013. 192p.