INSTITUTO FEDERAL
SANTA CATARINA

CÂMPUS FLORIANÓPOLIS
DEPARTAMENTO ACADÊMICO DE SAÚDE E SERVIÇOS
CURSO SUPERIOR DE TECNOLOGIA EM GESTÃO EM TECNOLOGIA DA INFORMAÇÃO

LEONARDO SALOMONE DE ABREU

Política de Segurança da Informação: desenvolvimento e aplicabilidades em empresas de pequeno porte

Florianópolis - SC
2022

Ficha de identificação da obra elaborada pelo autor.

Abreu, Leonardo Salomone de
Política de Segurança da Informação: desenvolvimento **e aplicabilidades / Leonardo Salomone de Abreu;** orientação **de Hamilcar Boing; coorientação de Egon Sewald** Junior. **- Florianópolis, SC,** 2022.
68 p.

Trabalho de Conclusão de Curso (TCC) - Instituto Federal **de Santa Catarina, Câmpus** Florianópolis. CST **em Gestão da Tecnologia da** Informação. Departamento **Acadêmico de Saúde e** Serviços.
Inclui Referências.

1. Segurança da informação. 2. Plano de contingência. **3. Gestão de risco. 4.** Tecnologia da informação. **I. Boing, Hamilcar. II. Junior, Egon Sewald. III.** Instituto **Federal de Santa Catarina. IV.** Política de Segurança da Informação.

INSTITUTO FEDERAL DE SANTA CATARINA
DEPARTAMENTO ACADÊMICO DE SAÚDE E SERVIÇOS
CURSO SUPERIOR DE TECNOLOGIA EM GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

LEONARDO SALOMONE DE ABREU

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: DESENVOLVIMENTO E APLICABILIDADES EM EMPRESAS DE PEQUENO PORTE

Trabalho de Conclusão de Curso submetido ao Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina como parte dos requisitos para obtenção do título de Tecnólogo em Gestão da Tecnologia da Informação.

Professor Orientador:
Prof. Hamilcar Boing, Doutor.

Professor Coorientador:
Prof. Egon Sewald Junior, Doutor.

FLORIANÓPOLIS - SC
NOVEMBRO/2022

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: DESENVOLVIMENTO E APLICABILIDADES EM EMPRESAS DE PEQUENO PORTE

LEONARDO SALOMONE DE ABREU

Este trabalho foi julgado adequado para obtenção do Título de Tecnólogo em Gestão da Tecnologia da Informação e aprovado na sua forma final pela banca examinadora do Curso Superior de Tecnologia em Gestão da Tecnologia da Informação do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina.

Florianópolis-SC, 18 de novembro de 2022.

IFSC
Documento assinado digitalmente
EGON SEWALD JUNIOR
Data: 30/11/2022 15:41:46-0300
CPF: 007.730.849-24
Verifique as assinaturas em https://v.ifsc.edu.br

Prof. Egon Sewald Junior, Doutor.
Coordenador do CST em Gestão da Tecnologia da Informação
Instituto Federal de Santa Catarina

Banca Examinadora:

IFSC
Documento assinado digitalmente
HAMILCAR BOING
Data: 30/11/2022 14:32:31-0300
CPF: 743.217.229-34
Verifique as assinaturas em https://v.ifsc.edu.br

Prof. Hamilcar Boing, Doutor.
Orientador
Instituto Federal de Santa Catarina

IFSC
Documento assinado digitalmente
EGON SEWALD JUNIOR
Data: 12/12/2022 15:35:12-0300
CPF: 007.730.849-24
Verifique as assinaturas em https://v.ifsc.edu.br

Prof. Egon Sewald Junior, Doutor.
Coorientador
Instituto Federal de Santa Catarina

IFSC
Documento assinado digitalmente
ADRIANO HEIS
Data: 30/11/2022 16:52:04-0300
CPF: 955.690.149-34
Verifique as assinaturas em https://v.ifsc.edu.br

Prof. Adriano Heis, Mestre.
Instituto Federal de Santa Catarina

IFSC
Documento assinado digitalmente
FELIPE CANTORIO SOARES
Data: 12/12/2022 16:04:14-0300
CPF: 398.713.399-68
Verifique as assinaturas em https://v.ifsc.edu.br

Prof. Felipe Cantório Soares, Mestre.
Instituto Federal de Santa Catarina

AGRADECIMENTOS

Agradeço primeiramente à minha família, que sempre me apoiou e me incentivou.

Agradeço também aos meus colegas de classe, que sempre colaboraram comigo e se tornaram bons amigos;

A todo o corpo docente do curso, pelo conhecimento transmitido sempre de forma prestativa e descontraída;

E por último aos meus orientadores, professores Hamilcar e Egon, assim como aos demais membros da banca, professores Adriano e Felipe, por todo o esforço e suporte prestado durante as etapas do trabalho.

“A melhor maneira de prever o futuro é criá-lo.”

Peter Ferdinand Drucker, escritor.

RESUMO

O presente estudo tem como objetivo principal documentar o processo de desenvolvimento e implementação de uma Política de Segurança da Informação aplicável a uma empresa local de pequeno porte, alertando aos gestores sobre a necessidade de se manter uma gestão de segurança corporativa eficaz frente às ameaças digitais que surgem diariamente.

A Política de Segurança da Informação é um conjunto de regras e procedimentos que determinam o acesso, o controle e o tráfego da informação em uma organização.

Para isso, primeiramente buscou-se entender as principais propriedades que compõem o conceito de Segurança da Informação, assim como a estrutura da política em si, que é baseada principalmente nas normas ISO 27001 e 27002, padrões internacionais que ditam a gestão de Segurança da Informação.

O projeto foi executado através de um estudo de caso em uma empresa de pequeno porte local (cujo nome não foi citado por questões de sigilo) e é de cunho exploratório e aplicado, tendo como objetivo gerar conhecimento prático acerca do assunto.

Palavras-chave: segurança da informação, plano de contingência, gestão de risco, tecnologia da informação.

ABSTRACT

The present study seeks to document the process of development and implementation of an Information Security Policy in a small local business, alerting managers of the need for an effective corporate security management against the digital threats that emerge everyday.

An Information Security Policy is a set of rules and procedures that shape the access, control and traffic of information inside an organization.

In order to achieve this, firstly we seek to understand the main concepts that compose Information Security as a whole, as well as the Information Security Policy structure, which is heavily based on the 27001 and 27002 ISO's, international standards that dictate the Information Security management.

The project was carried out through a case study ran in a small local company (whose name is not mentioned for confidentiality reasons) and is considered exploratory and applied, therefore aiming to generate practical knowledge on the subject.

Keywords: information security, contingency plan, risk management, information technology.

LISTA DE ILUSTRAÇÕES

Figura 1 – Exemplo de email contendo fraude de *phishing*…… 19
Figura 2 – Camadas de Segurança da Informação…… 20
Figura 3 – Componentes da política…… 22
Figura 4 – Modelo de Política de Segurança da Informação…… 24
Figura 5 – Etapas da pesquisa…… 26
Figura 6 – Conceitos de Segurança da Informação…… 26
Figura 7 – Estrutura da Política de Segurança da Informação…… 27
Figura 8 – Diagrama de diagnóstico da empresa…… 27
Figura 9 – Fluxograma de elaboração da política…… 28
Figura 10 – Cartilha de boas práticas em redes sociais…… 40

LISTA DE ABREVIATURAS E SIGLAS

CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CGSI	Comitê Gestor de Segurança da Informação
IFSC	Instituto Federal de Santa Catarina
ISO	*International Organization for Standardization* (Organização Internacional de Normalização)
NBR	Norma Brasileira
PGSI	Política Geral de Segurança da Informação
TI	Tecnologia da Informação
UDESC	Universidade do Estado de Santa Catarina
UFSC	Universidade Federal de Santa Catarina

SUMÁRIO

1. INTRODUÇÃO.....14

1.1. JUSTIFICATIVA.....14

1.2. DEFINIÇÃO DO PROBLEMA.....15

1.3. OBJETIVOS.....15

1.3.1. OBJETIVO GERAL.....15

1.3.2. OBJETIVOS ESPECÍFICOS.....15

1.4. ESTRUTURA DO TRABALHO.....16

2. REVISÃO DA LITERATURA.....17

2.1. PROPRIEDADES BÁSICAS DA SEGURANÇA DA INFORMAÇÃO.....17

2.2. PLANO DE SEGURANÇA DA INFORMAÇÃO E ASPECTOS RELACIONADOS.....21

2.3. ESTRUTURA DO PLANO DE AÇÃO.....22

3. PROCEDIMENTOS METODOLÓGICOS.....25

3.1. CARACTERIZAÇÃO DA PESQUISA.....25

3.2. DELIMITAÇÃO E POPULAÇÃO DA PESQUISA.....26

3.3. ETAPAS DA PESQUISA.....26

4. DESENVOLVIMENTO E IMPLEMENTAÇÃO DO PLANO GERAL DE SEGURANÇA DA INFORMAÇÃO.....29

4.1. CONTATO INICIAL.....29

4.2. DIAGNÓSTICO DA EMPRESA.....29

4.2.1. PERFIL DOS FUNCIONÁRIOS.....29

4.2.2. INFRAESTRUTURA DA EMPRESA.....30

4.2.3. HISTÓRICO DE INCIDENTES.....30

4.3. ELABORAÇÃO DA POLÍTICA.....31

4.3.1. POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO.....31

4.3.1.1 INTRODUÇÃO.....31

4.3.1.2 PROPÓSITO.....31

4.3.1.3 ESCOPO.....32

4.3.1.4 DIRETRIZES.....32

4.3.1.5 PAPÉIS E RESPONSABILIDADES....32
4.3.1.6 SANÇÕES, PUNIÇÕES E CASOS OMISSOS....33
4.3.1.7 GLOSSÁRIO....34
4.3.1.8 REVISÕES E GESTÃO DA POLÍTICA....34
4.3.2. EQUIPAMENTOS COMPUTACIONAIS....34
4.3.3. MONITORAMENTO....35
4.3.4. EMAIL E COMUNICADORES INSTANTÂNEOS....35
4.3.5. INTERNET E MÍDIAS SOCIAIS....36
4.3.6. CÓDIGOS MALICIOSOS....36
4.3.7. ACESSO REMOTO....37
4.3.8. RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO....37
4.3.9. *BACKUP* E RESTAURAÇÃO DE DADOS....37
4.3.10. TERMO DE USO INTERNO....38
4.4. ADEQUAÇÃO, APROVAÇÃO E DIVULGAÇÃO....39
4.5. AVALIAÇÃO....40
5. CONCLUSÕES....42
5.1. EM RELAÇÃO AO OBJETIVO GERAL....42
5.2. EM RELAÇÃO AOS OBJETIVOS ESPECÍFICOS....42
5.3. TRABALHOS FUTUROS....43
REFERÊNCIAS....44
APÊNDICE A – POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO....48
APÊNDICE B – NORMA DE ATIVOS DE INFORMAÇÃO....52
APÊNDICE C – NORMA DE USO DE EQUIPAMENTOS COMPUTACIONAIS PESSOAIS 55
APÊNDICE D – NORMA DE MONITORAMENTO....57
APÊNDICE E – NORMA DE COMPORTAMENTO EM SERVIÇOS DE EMAIL E COMUNICADORES INSTANTÂNEOS....59
APÊNDICE F – NORMA DE COMPORTAMENTO NA INTERNET E MÍDIAS SOCIAIS..61
APÊNDICE G – NORMA DE CÓDIGOS MALICIOSOS....63
APÊNDICE H – NORMA DE ACESSO REMOTO....65

APÊNDICE I – NORMA DE RESPOSTA A INCIDENTES.....67

APÊNDICE J – TERMO DE USO INTERNO.....68

1. INTRODUÇÃO

Este capítulo apresenta a justificativa de escolha do tema do trabalho, destacando a importância de se manter uma Política de Segurança de Informação em uma organização e apresentando a questão norteadora do projeto, tal como sua estrutura.

1.1. JUSTIFICATIVA

Considerando o valor da informação em uma organização na atualidade, se dá necessário protegê-la devidamente, garantindo a integridade da mesma (FONTES, 2006). Contudo, o crescente número de ataques demonstra a ineficácia dos mecanismos de defesa correspondentes, frente às milhares de ameaças que surgem todos os dias.

Para controlar tais riscos, é necessário elaborar uma gestão dos riscos tecnológicos e mantê-la constantemente atualizada, seguindo boas práticas a serem empregadas desde o planejamento à manutenção dos Sistemas de Informação (HORI, 2003).

A Política de Segurança da Informação é um conjunto de documentos que dita normas e diretrizes de uso no que diz respeito aos ativos de Tecnologia da Informação.

Ela tem como objetivo a preservação da confidencialidade, integridade e disponibilidade da informação (ISO 27000:2016), a fim de assegurar o sucesso e a continuidade do negócio, assim como minimizar as consequências dos incidentes de Segurança da Informação.

Dessa forma, considera-se como útil ao curso e à sociedade a documentação do processo de desenvolvimento do Plano de Segurança da Informação em uma organização.

Em relação aos objetivos do curso de Gestão em Tecnologia da Informação, podemos recorrer ao Plano Pedagógico do Curso, onde são apresentados alguns itens que se relacionam com o tema do presente trabalho, justificando a pesquisa:

- A formação de recursos humanos para o gerenciamento das tecnologias da informação, com vistas a atender as necessidades da sociedade;
- Capacitar profissionais para o planejamento da infraestrutura tecnológica de empresas, orientando a aplicação tanto ao ambiente organizacional interno, como ao ambiente externo;
- Desenvolver visão e raciocínio estratégico para a definição e implementação dos princípios de gestão das tecnologias da informação;

• Disseminar conhecimentos tecnológicos e gerenciais que possibilitem ao aluno conduzir projetos, programas e atividades de aplicação das tecnologias da informação com qualidade e segurança;

• Conhecer e aplicar técnicas de administração e gerência para a área de Tecnologia de Informação.

De acordo com um estudo realizado pela seguradora JLT, com 196 empresas de médio e grande porte, o número de empresas que afirmam ter sido vítimas de ciberataques passou de 25% em 2017 para 34,71% em 2018, o que mostra a ineficácia da gestão de segurança corporativa frente às novas ameaças digitais.

Sendo assim, o trabalho se propõe a desenvolver uma Política de Segurança da Informação em uma organização e avaliar o efeito causado pela falta dela em suas operações de negócio, expondo aos gestores a necessidade de se rever as práticas e mecanismos de defesa da empresa em relação aos seus recursos tecnológicos.

1.2. DEFINIÇÃO DO PROBLEMA

Tendo em vista a dependência da Tecnologia da Informação por parte das organizações no mercado atual, além do crescente número de ciberataques e vazamento de dados, se dá como necessário uma forma de protegê-la.

De tal forma, temos a seguinte pergunta como norteadora desta pesquisa: "Como desenvolver e implementar uma Política de Segurança da Informação em uma empresa de pequeno porte?”

1.3. OBJETIVOS

Para o desenvolvimento deste trabalho foram definidos os seguintes objetivos: geral e específicos.

1.3.1. OBJETIVO GERAL

Propor a Política Geral de Segurança da Informação em uma empresa de pequeno porte.

1.3.2. OBJETIVOS ESPECÍFICOS

- Identificar as principais ameaças de Segurança da Informação, assim como suas respectivas ferramentas e estratégias de defesa;

- Identificar as atividades que compõem o Plano de Segurança da Informação;
- Desenvolver e implementar um Plano de Segurança da Informação aplicável a empresas de pequeno porte.

1.4. ESTRUTURA DO TRABALHO

O trabalho está estruturado em cinco capítulos:

O primeiro capítulo introduz o tema e apresenta a justificativa do trabalho, assim como a problemática de pesquisa e a definição dos objetivos geral e específicos;

O segundo capítulo trata do embasamento teórico do trabalho, introduzindo e conceituando os temas relevantes ao seu desenvolvimento;

O terceiro capítulo apresenta o procedimento metodológico adotado, tal como as etapas de execução da pesquisa;

O quarto capítulo contém o desenvolvimento propriamente dito da pesquisa, detalhando a obtenção dos dados assim como as ações tomadas para a resolução dos problemas encontrados;

O quinto capítulo apresenta as conclusões do trabalho em relação aos objetivos.

2. REVISÃO DA LITERATURA

2.1. PROPRIEDADES BÁSICAS DA SEGURANÇA DA INFORMAÇÃO

Com o avanço tecnológico, a informação tornou-se um bem muito valioso e de grande valor estratégico, desempenhando um importante papel no âmbito organizacional e servindo como ferramenta estratégica no apoio à tomada de decisões, assim como auxílio aos gestores na análise de riscos e na criação de novos produtos.

Nesse cenário, fica evidente a dependência das empresas em relação à informação, que se torna muito mais digitalizada, compartilhada e distribuída (SÊMOLA, 2003).

Conforme descrito por Mitnick e Simon (2006), muitas empresas sobrevivem após terem suas fábricas queimadas ou após a saída de funcionários-chave. Entretanto, a perda de propriedade intelectual é algo totalmente diferente. Se você tem seus designs de produto, dados de pesquisa e desenvolvimento ou lista de clientes roubada, esse sim seria um golpe que poderia levar sua empresa à falência.

Sendo assim, ela deve ser devidamente protegida (FONTES, 2008), a fim de evitar incidentes que possam ser prejudiciais aos processos de negócios, como indisponibilidade, perda, acesso e/ou alteração indevida da informação – além de maximizar o retorno sobre os investimentos e oportunidades de negócio em uma organização (NBR ISO/IEC 27002:2005).

Segundo a norma ISO/IEC 17799, a Segurança da Informação se apoia em quatro principais pilares, sendo eles:

Integridade: A informação deve manter todas as características originais estabelecidas pelo seu proprietário, incluindo controle de mudanças e garantia do seu ciclo de vida;

Confidencialidade: O acesso à informação deve ser limitado apenas às entidades devidamente autorizadas pelo proprietário da mesma;

Disponibilidade: A informação deve estar sempre disponível para uso legítimo, ou seja, pelas entidades autorizadas;

Autenticidade: A informação não deve ter sido alterada em relação à sua fonte de origem.

Entretanto, Castro (2010) acredita que a fragilidade dos processos de proteção tem avançado na mesma proporção com que as ameaças surgem e os considera como a real dimensão dos perigos na segurança organizacional.

Pode-se considerar como ameaça todo e qualquer elemento que tem condição de explorar vulnerabilidades e causar problemas aos ativos em uma organização (ANDERSON, 2006).

Vulnerabilidades são deficiências de diversas origens, que muitas vezes não são identificadas a tempo ou devidamente tratadas de modo a evitar um ataque (NAKAMURA, 2002).

Os indivíduos que invadem sistemas computacionais e exploram suas vulnerabilidades, obtendo ou não êxito, são chamados de atacantes (NAKAMURA, 2002), mais conhecidos como *hackers*.

Existem diversas categorias de *hackers*, e dentre elas se destacam as seguintes:

Crackers: *Hackers* que possuem conhecimento avançado e o utilizam para quebrar a segurança de informações e anular sistemas;

Responsáveis por invasões ***ransomware***, meio de ataque que age como uma forma de sequestro, impedindo a vítima de acessar seu sistema e/ou arquivos pessoas, na maioria dos casos exigindo um pagamento em troca do acesso.

O relatório SonicWall de ameaças cibernéticas revelou que, em 2022, o Brasil sofreu mais de 33 milhões de tentativas de *ransomware* e, de acordo com o departamento de pesquisa Statista, em 2021 o tempo médio de inatividade de uma empresa que sofreu esse tipo de ataque foi de 22 dias.

Phishers: Hackers que praticam o *phishing*, forma de ataque muito comum baseada em engenharia social, que utiliza-se de emails e/ou sites falsos, levando a vítima a revelar informações pessoais como CPF e/ou senhas de contas bancárias;

À primeira vista podem parecer mensagens legítimas, informando supostas implicações na conta da vítima ou solicitando uma atualização de cadastro, por exemplo.

A vítima então é redirecionada a uma página falsa, muitas vezes idêntica à original, onde tem suas informações roubadas.

Figura 1 – Exemplo de email contendo fraude de *phishing*



Fonte: Dinamio (2020)

Para evitar esse tipo de ataque, o usuário deve atentar-se quanto ao domínio e ao endereço de email em questão, verificando se os mesmo são legítimos.

No exemplo acima, a fraude pode ser identificada através do endereço de email, que é falso (@olines.com.br, ao invés de @bb.com.br).

Ainda assim, é importante notar que, em muitos casos, o domínio ou endereço de email pode ser muito parecido com o real, mesmo sendo falso.

Isso pode ser alcançado de diversas formas, como utilizando um domínio homóglifo (“facebóók”, “brade5co”, “paypal” [com “i” maiúsculo]) ou um subdomínio alternativo (“www.santander-com.xyz”).

Insiders: Ex-colaboradores ou colaboradores insatisfeitos em organizações com acesso a informações sigilosas que decidem apropriar-se indevidamente delas, seja com a finalidade de vendê-las ou apenas para prejudicar a empresa.

Um estudo do Centro de Inteligência em Segurança da IBM relatou que, em 2015, 60% dos ataques registrados aconteceram pelo lado de dentro da rede, o que demonstra o quão fácil pode ser efetuar uma invasão, uma vez que dentro dela.

Os ataques podem ocorrer quando as vulnerabilidades de segurança não são tratadas (NAKAMURA, 2002), tendo origem através das ameaças, que são classificadas por Sêmola (2003) de três formas:

Intencionais: Ameaças propositais, como crackers, insiders, roubo e vandalismo;

Involuntárias: Falhas não intencionais, como falta de conhecimento, falta de energia ou acidentes;

Naturais: Condições da natureza que podem causar danos à segurança da informação, como tempestades, incêndios, enchentes e terremotos.

Entretanto, ao contrário do que se pode imaginar, a Segurança da Informação não limita-se ao nível lógico.

Adachi (2004) divide o assunto em três camadas:

Figura 2 – Camadas de Segurança da Informação



Fonte: Teleco (2012)

Na camada **física** está contido o ***hardware***, que fica descrito por Keen (1996) como um conjunto de unidades que constituem um sistema de processamento de dados;

Nela estão compreendidos os aspectos relacionados ao ambiente físico da organização, abrangendo desde sua localização até sua estrutura de cabeamento, instalação elétrica e sistema de climatização.

Já a camada **lógica** é composta pelo ***software***, conjunto de instruções arranjadas logicamente a serem interpretadas e executadas pelo hardware para resolver uma aplicação específica (PRESSMAN, 2006);

No âmbito de segurança, é nessa camada que encontram-se os mecanismos de defesa responsáveis por resguardar os ativos de informação, como antivírus, *firewall*, protocolos de criptografia e ferramentas de *backup*, controle de acesso e monitoramento, por exemplo.

A camada **humana**, por sua vez, é formada pelas **pessoas**, sendo inevitavelmente o elo mais fraco no ciclo da segurança, de acordo com Schneier (2001);

Aqui contemos os procedimentos que apoiam a Segurança da Informação, como a gestão de risco, os treinamentos, a conscientização dos colaboradores e a própria Política de Segurança da Informação.

Dessa forma, fica claro que a Segurança da Informação deve abordar as três camadas, de forma a prover uma composição de agentes que torne a estrutura mais segura (BEZERRA, 2015).

2.2. PLANO DE SEGURANÇA DA INFORMAÇÃO E ASPECTOS RELACIONADOS

A Política de Segurança da Informação é uma declaração formal da organização acerca de seu compromisso com a proteção das informações de sua propriedade ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores, com o propósito de estabelecer diretrizes, procedimentos e mecanismos relacionados à Segurança da Informação.

Lyra (2008, p. 149) acredita que o plano deve orientar sobre como a organização se portará frente à Segurança da Informação, e que cada organização deve produzir um Plano Diretor de Segurança específico, de acordo com suas necessidades, ameaças, vulnerabilidades e exposição ao risco.

Portanto, podemos considerar o Plano de Segurança da Informação como um recurso estratégico, servindo como documento norteador e definindo as políticas de segurança em uma empresa, a fim de garantir a proteção de seus ativos de informação.

A política deve prover apoio à Segurança da Informação de acordo com os requisitos do negócio e regulamentações relevantes e incluir seus objetivos, fornecendo uma estrutura para estabelecê-los.

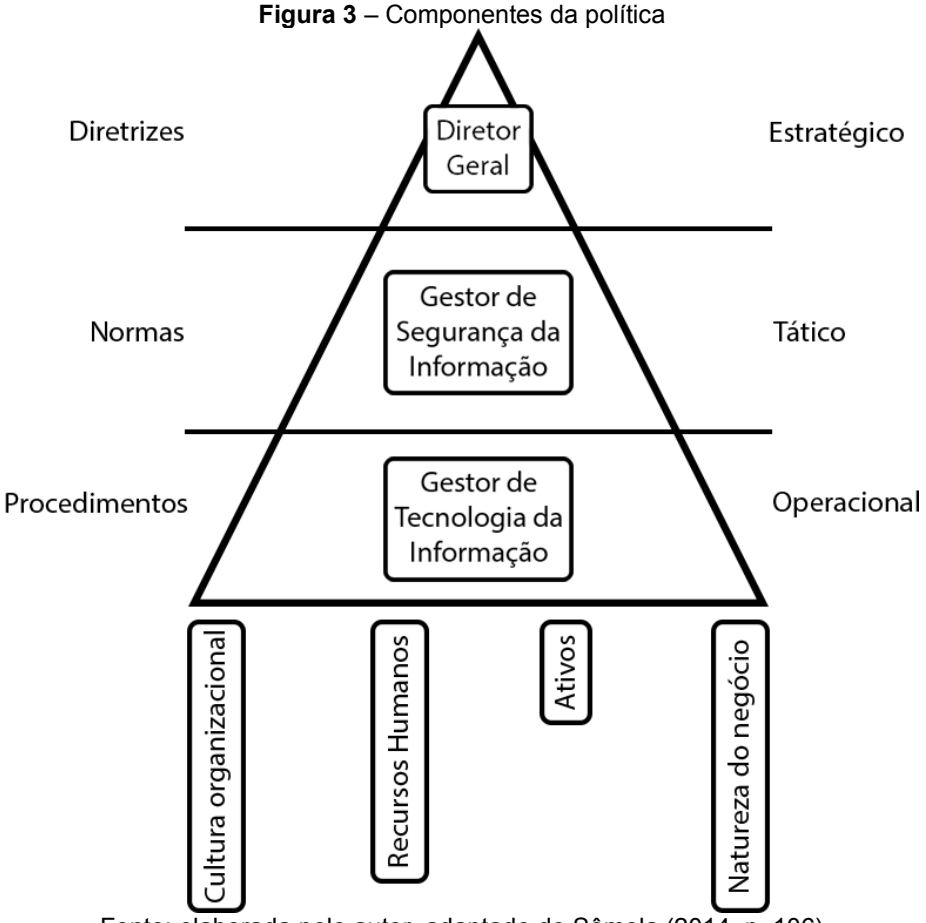
Além disso, deve ser garantida a publicação e divulgação adequada para os colaboradores e quaisquer outras partes externas relevantes, assim como o comprometimento com as diretrizes estabelecidas.

2.3. ESTRUTURA DO PLANO DE AÇÃO

O Plano de Segurança da Informação varia de organização para organização, de acordo com a área de atuação, cultura organizacional, grau de informatização, perfil dos funcionários e outros aspectos.

Entretanto, Sêmola (2014, p. 106) classifica os componentes da política em três níveis de sustentação:

Figura 3 – Componentes da política



Fonte: elaborada pelo autor, adaptado de Sêmola (2014, p. 106)

Analisando a figura, vemos que o autor entende que a Política de Segurança da Informação deve conter diretrizes gerais no nível estratégico da empresa, que são compostas por normas no nível tático, que por sua vez são executadas através de procedimentos e instruções no nível operacional da organização.

Para facilitar o entendimento dessa abordagem, podemos definir uma pergunta norteadora para cada componente, considerando-os da seguinte forma:

Diretrizes: “O quê deve ser feito?”

Normas: “Quais são as regras?”

Procedimentos e instruções: “Como fazer?”

Além disso, segundo a NBR:ISO 17799, a Política de Segurança da Informação deve abordar alguns pontos para garantir que seu sucesso seja atingido.

Nesse contexto, podemos destacar:

Tabela 1 – Estrutura recomendada da Política de Segurança da Informação

Política de Segurança da Informação	
Capítulo	**Objetivo**
Introdução	Estabelecer os objetivos da política
Escopo	Definir a quem ela se destina
Diretrizes	Detalhar as normas e critérios estabelecidos
Gestão de continuidade	Definir o curso de ação a ser tomado no caso de incidentes de segurança da informação
Sanções e punições	Explicitar as sanções a serem aplicadas no caso do descumprimento com as normas
Revisões	Definir o período de revisão dos documentos
Gestão da política	Formalizar o comprometimento da alta direção com as metas e princípios estabelecidos

Fonte: elaborada pelo autor, adaptado da NBR:ISO 17799

Como exemplo, podemos utilizar a Política de Segurança e Privacidade da Informação da Unimed, confederação que atua como operadora de planos de saúde.

A última revisão da política foi publicada em 2021 e pode ser encontrada diretamente no portal da empresa.

Aqui podemos visualizar toda a estrutura recomendada descrita, aplicada de forma prática:

Figura 4 – Modelo de Política de Segurança da Informação

Unimed Norte Pioneiro-PR	Título: POLÍTICA DE SEGURANÇA E PRIVACIDADE DA INFORMAÇÃO	Código do Procedimento: POL-TI-001
Número de Revisão: 6	Data de Revisão: 30/11/2021	Página: 3 / 15
Elaboração: Crislayne Maria Durante de Oliveira	Aprovação: Wellington Luiz Francisquini	

Abrangência

Todos os setores da organização

Da Aplicação

Os itens estabelecidos na Política de Segurança da Informação e Privacidade da Informação são aplicáveis a todos os colaboradores, processos de negócio e sistemas de informação que manipulam direta ou indiretamente as informações de propriedade ou sob custódia da Unimed Norte Pioneiro-PR, independentemente do local e da forma como estejam armazenadas, contidas ou distribuídas na cooperativa. Todos os colaboradores devem ter acesso a esta política, não sendo admitido o desconhecimento de seu conteúdo para justificar violações ou descumprimento das diretrizes estabelecidas.

A Política de Segurança e Privacidade da Informação, bem como, o Termo de Responsabilidade de Segurança da Informação são explanados em sua íntegra à todo colaborador, após sua contratação, por meio de uma reunião para apresentação das políticas gerais da Cooperativa. A aplicação destes termos é feita impreterivelmente pelo setor de Tecnologia da Informação.

Diretrizes Gerais

Quanto à Informação:

□□A Unimed Norte Pioneiro-PR tem políticas documentadas que contemplam a segurança e a proteção da confidencialidade da informação clínica de seus beneficiários e de todos os dados pessoais que possam causar riscos ou danos, inclusive morais aos mesmos;

□□Toda e qualquer informação somente deve ser utilizada pelo colaborador para fins profissionais, não sendo permitida a divulgação de informações sigilosas e documentos. Casos de exceções deverão ser autorizados pelos gerentes ou proprietários da informação, e/ou ainda, sob determinação jurídica;

Fonte: Unimed (2021, p. 3)

3. PROCEDIMENTOS METODOLÓGICOS

O tópico a seguir tem como objetivo definir a metodologia a ser utilizada na pesquisa, bem como descrever as ferramentas que serão utilizadas na condução da pesquisa e na análise de seus resultados.

3.1. CARACTERIZAÇÃO DA PESQUISA

Ao realizar uma pesquisa científica, faz-se necessário traçar claramente os procedimentos metodológicos a serem utilizados, de forma a alcançar os objetivos desejados.

Sendo assim, a presente pesquisa fica especificada em quatro pontos:

a) Quanto à sua **natureza**, a pesquisa caracteriza-se como **aplicada**, tendo como objetivo obter mais informações sobre o assunto e gerar conhecimento prático;

b) Quanto aos seus **objetivos**, a pesquisa é definida como **exploratória**, buscando proporcionar maior familiaridade com o problema e de forma a torná-lo mais explícito, de acordo com Gil (2002);

c) Ademais, levando em conta a problemática da pesquisa, o trabalho emprega uma **abordagem qualitativa**, envolvendo a obtenção de dados descritivos obtidos no contato direto do pesquisador com a situação estudada (BOGDAN E BIKLEN, 1982);

d) Por último, quanto aos **procedimentos**, foi definida a execução do trabalho através de um **estudo de caso**, que fica descrito por Yin (2005, p. 19) como uma "investigação empírica de um fenômeno contemporâneo dentro de um contexto da vida real", fomentando relatos e levantando fatores relevantes no processo de implementação de um Plano de Segurança da Informação em uma organização, conforme os objetivos propostos.

3.2. DELIMITAÇÃO E POPULAÇÃO DA PESQUISA

A pesquisa foi feita em uma empresa de pequeno porte na área de desenvolvimento de softwares para varejo, situada na região de Santa Catarina.

A organização está no mercado há mais de vinte anos e atualmente conta com seis funcionários: um responsável comercial, dois técnicos de suporte, dois desenvolvedores e um diretor administrativo.

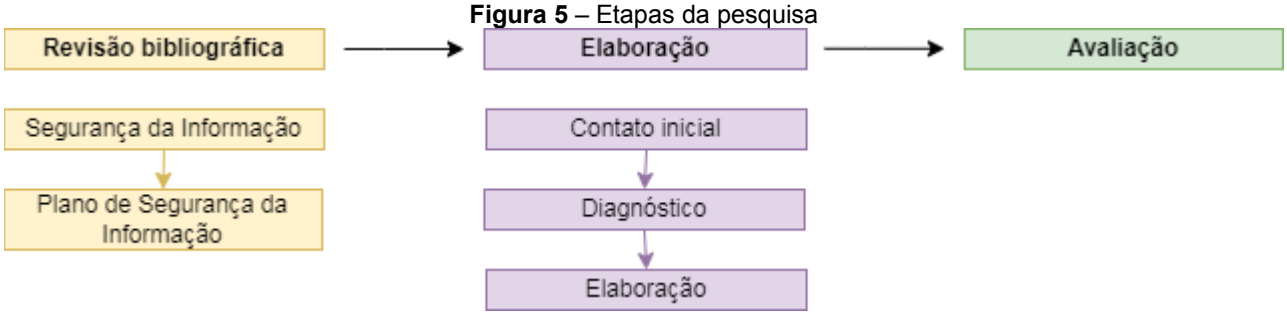
A empresa gerencia diversos dados fiscais sensíveis e possui uma carteira de clientes seleta, composta de aproximadamente duzentos comércios ativos.

Por questões de sigilo, optou-se por não citar o nome da empresa.

3.3. ETAPAS DA PESQUISA

A pesquisa foi dividida em três principais etapas: revisão bibliográfica, elaboração e avaliação.

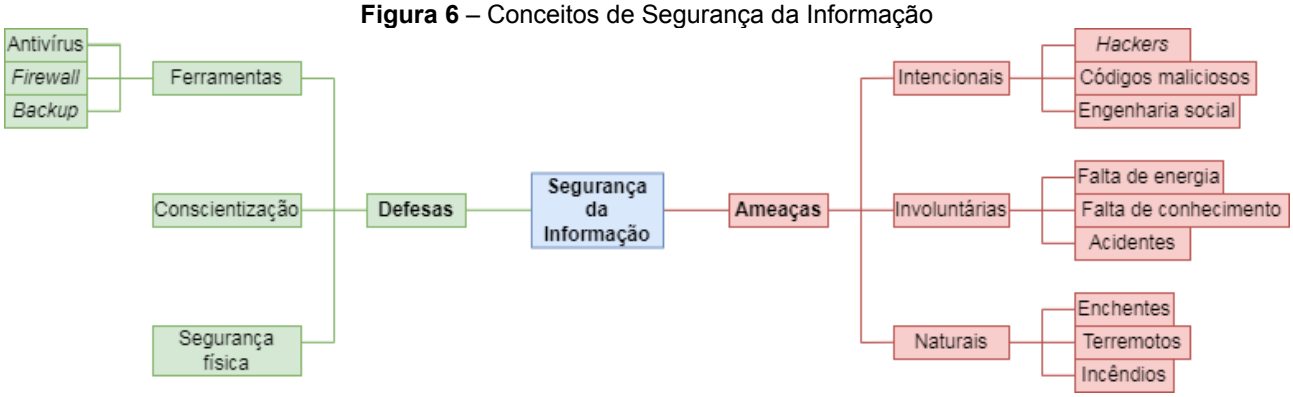
Figura 5 – Etapas da pesquisa



Fonte: elaborada pelo autor

Na primeira etapa, foi feita uma revisão bibliográfica acerca do assunto, onde foram identificadas as principais ameaças no que diz respeito à Segurança da Informação, assim como seus respectivos mecanismos de defesa.

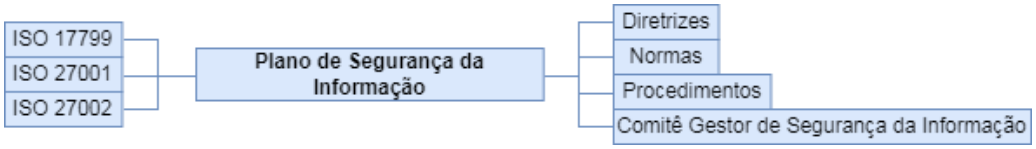
Figura 6 – Conceitos de Segurança da Informação



Fonte: elaborada pelo autor

Além disso, nessa etapa encontrou-se também a existência de um instrumento já reconhecido que formaliza a Segurança da Informação em uma organização, tornando-se o objetivo principal da pesquisa.

Figura 7 – Estrutura da Política de Segurança da Informação



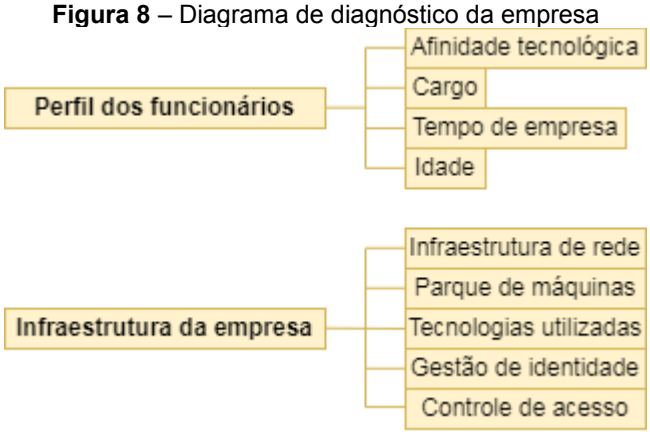
Fonte: elaborada pelo autor

A partir de então, iniciou-se o processo de elaboração da Política de Segurança da Informação, este sendo dividido em três sub-etapas: contato inicial, diagnóstico da empresa e elaboração do plano.

No contato inicial, foi apresentada a proposta da pesquisa à diretoria executiva da organização.

Após o aceite da proposta, foi feito um diagnóstico da empresa através de um mapeamento do perfil dos funcionários, assim como um levantamento de sua infraestrutura.

Figura 8 – Diagrama de diagnóstico da empresa

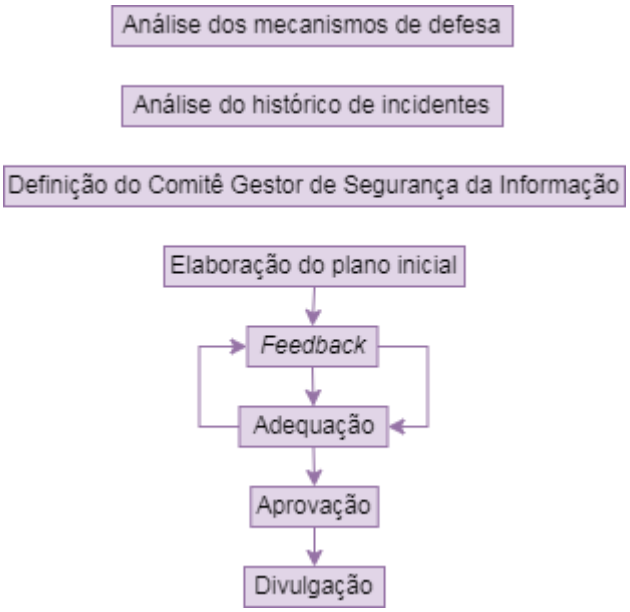


Fonte: elaborada pelo autor

Já a elaboração iniciou com uma análise da empresa, a fim de medir seu nível de maturidade em Segurança da Informação, chegando na definição do Comitê Gestor de Segurança da Informação – corpo responsável pela elaboração, aprovação e manutenção das diretrizes e normas estabelecidas.

A partir de então, iniciou-se a confecção propriamente dita dos documentos, que posteriormente passaram por um *feedback* da alta diretoria e foram adequados conforme as realidades da empresa, para poderem por fim receber sua aprovação e serem devidamente divulgados, sendo colocados em prática.

Figura 9 – Fluxograma de elaboração da política



Fonte: elaborada pelo autor

Por fim, após a divulgação dos documentos, foi feita a análise dos resultados a partir de uma avaliação da política, feita por um especialista na área.

4. DESENVOLVIMENTO E IMPLEMENTAÇÃO DO PLANO GERAL DE SEGURANÇA DA INFORMAÇÃO

Passado o levantamento do referencial teórico e a definição das etapas da pesquisa, buscou-se executá-las.

Sendo assim, neste capítulo fica descrito o processo de desenvolvimento e implementação do Plano de Segurança da Informação na organização em questão, de acordo com as etapas propostas.

4.1. CONTATO INICIAL

Nesta etapa, foi convocada uma reunião com a diretoria executiva da organização, composta pelo diretor geral e pela diretora administrativa da empresa, onde foi apresentada a proposta do projeto, expondo aos gestores os riscos e as necessidades de se estabelecer tais diretrizes e normas, a fim de garantir a segurança de seus recursos tecnológicos e principalmente dos ativos de informação frente ao mercado.

Buscou-se utilizar uma abordagem lúdica e descontraída, de forma a facilitar o entendimento de todas as partes.

A diretoria brevemente entendeu a necessidade, assim como os riscos aos quais a empresa estava correndo e mostrou-se interessada, aceitando a proposta.

4.2. DIAGNÓSTICO DA EMPRESA

Após o aceite da proposta, buscou-se fazer um diagnóstico da empresa, levantando informações pertinentes à elaboração do plano.

Dentre as informações levantadas, cita-se como as mais relevantes:

4.2.1. PERFIL DOS FUNCIONÁRIOS

O perfil médio dos funcionários está na faixa etária dos 25 a 40 anos, oscilando de 1 a 12 anos de empresa (desconsiderando o diretor geral, fundador da empresa). Além disso, todos os funcionários possuem alta afinidade tecnológica (devido ao segmento no qual a empresa está inserida, além de fatores como formação acadêmica e vasta experiência profissional na área de tecnologia).

4.2.2. INFRAESTRUTURA DA EMPRESA

O escritório está localizado em um edifício comercial, contendo portaria com acesso controlado e monitorado por um circuito interno de câmeras. O acesso à sala é controlado por um leitor de impressões digitais.

Já o parque ativo de máquinas da empresa conta com 8 computadores (incluindo o servidor), todos equipados com sistema operacional Windows sempre atualizado e antivírus licenciado.

O servidor é desligado à noite e nos finais de semana, a fim de evitar possíveis ataques.

A empresa não possui um plano de contingência explicitamente estabelecido, apenas um código de conduta profissional, que estabelece de forma abstrata algumas diretrizes relevantes à segurança da informação, como impedir prejuízos materiais à empresa ou danos à sua imagem, limitar o acesso de informações de propriedade da empresa e impedir a cópia ou divulgação das mesmas.

Ademais, as senhas dos computadores, contas de email e diretório de arquivos seguem um padrão, composto por uma combinação entre uma sequência numérica, a abreviação do departamento e um caractere especial.

4.2.3. HISTÓRICO DE INCIDENTES

Ao questionar o desenvolvedor sênior sobre o histórico de incidentes de Segurança da Informação na empresa, o mesmo recordou-se de apenas um episódio, ocorrido em meados de 2015 ou 2016, onde a organização foi vítima de um *ransomware* que infectou o servidor e criptografou diversos arquivos, atacando principalmente documentos de texto e planilhas.

O funcionário explicou também que grande parte dos arquivos foram recuperados pois a empresa possui uma rotina de backup ativa que compacta e criptografa as cópias, impedindo a recriptografia das mesmas, mas que, ainda assim, alguns documentos foram perdidos permanentemente.

4.3. ELABORAÇÃO DA POLÍTICA

Passada a etapa de diagnóstico da empresa, partiu-se para o desenvolvimento propriamente dito do plano, levando em consideração as informações levantadas nas etapas anteriores.

A elaboração da primeira revisão do Plano de Segurança da Informação foi feita com base no minicurso ISO 27001: Construindo Políticas de Segurança da Informação, ministrado por Cláudio Dodt – especialista no segmento com mais de 15 anos de atuação.

O curso aborda conceitos que vão desde a conscientização da necessidade até a garantia da conformidade com a política e disponibiliza modelos base para a elaboração de um plano, que serviram como ponto de início aqui.

Além disso, a política apoia-se também na Cartilha de Segurança para Internet (disponível em https://www.cartilha.cert.br), material produzido pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil que recomenda boas práticas em Segurança da Informação.

4.3.1. POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

A elaboração dos documentos foi concebida de acordo com a estrutura recomendada pela NBR:ISO 17799 (abordada no capítulo 2.3), a partir dos modelos disponibilizados no curso.

Sendo assim, o documento principal, encontrado no apêndice A, contém:

4.3.1.1 INTRODUÇÃO

Aqui introduzimos a missão da empresa e estabelecemos a Política de Segurança da Informação como recurso estratégico na gestão corporativa da empresa, tendo como objetivo garantir os níveis adequados de proteção às informações da organização.

4.3.1.2 PROPÓSITO

Neste capítulo explicamos o propósito da PGSI, que tem como objetivo:

• Adotar padrões de comportamento seguro;

• Orientar na adoção de controles e processos para cumprimento dos requisitos estabelecidos;

• Resguardar os ativos de informação da empresa, garantindo os requisitos dos quatros requisitos básicos de segurança: confidencialidade, integridade e disponibilidade e autenticidade;

• Prevenir possíveis causas de incidentes de Segurança da Informação, minimizando o risco de perdas financeiras, participação de mercado ou qualquer outro impacto negativo à operação da empresa.

4.3.1.3 ESCOPO

No que tange ao escopo, definiu-se que a política se aplica a todos os usuários das informações da empresa – incluindo qualquer indivíduo ou organização que possui (ou possuiu) vínculo com a empresa e/ou fizeram, fazem ou farão uso dos recursos computacionais e informações de propriedade da mesma.

4.3.1.4 DIRETRIZES

Aqui apresentamos as principais diretrizes da empresa no que diz respeito à Segurança da Informação, sendo elas:

• Elaborar, implantar e seguir políticas, normas e procedimentos de Segurança da Informação, garantindo os requisitos básicos de segurança (confidencialidade, integridade e disponibilidade);

• Disponibilizá-las a todas as partes interessadas e autorizadas;

• Garantir a conscientização sobre as práticas adotadas;

• Atender aos requisitos aplicáveis ou exigidos pela legislação vigente;

• Investigar, corrigir e documentar possíveis incidentes de Segurança da Informação;

• Efetuar uma revisão sistemática dos objetivos, garantindo a melhoria contínua da Gestão de Segurança da Informação.

4.3.1.5 PAPÉIS E RESPONSABILIDADES

Durante o desenvolvimento de um Plano de Segurança da Informação, Ferreira e Araújo (2014, p.37) recomendam a definição de um Comitê Gestor de Segurança da Informação – corpo responsável por propor, implementar e garantir o cumprimento das normas estabelecidas.

Os autores sugerem que o comitê seja “constituído por profissionais de diversos departamentos, como, por exemplo, informática, jurídico, auditoria, engenharia”, e que ele deva catalogar todas as informações da organização, agrupando-as por categorias.

Entretanto, devido ao seu porte, na empresa em questão alguns desses cargos sequer existem (e, portanto, ficam sob responsabilidade do diretor geral).

Dessa forma, o Comitê Gestor de Segurança da Informação ficou composto pelo analista de suporte (que fará o papel do Gestor de Segurança da Informação) juntamente ao desenvolvedor sênior (responsável informal pelo setor de Tecnologia da Informação), assim como pelo diretor geral da organização.

Na PGSI, o comitê como um todo deve promover a divulgação da mesma, disseminando uma cultura de segurança no ambiente corporativo através da adoção de um padrão de comportamento seguro por seus colaboradores;

Para mais, cada membro da equipe tem suas respectivas responsabilidades:
O Gestor de Segurança da Informação age como peça chave na política, tendo como principal papel implantar e fazer cumprir as diretrizes estabelecidas.

Já o Gestor de Tecnologia da Informação gerencia os procedimentos e ferramentas necessárias para se alcançar os níveis de segurança definidos.

O Diretor Geral, por sua vez, é o responsável por apoiar e prover os recursos necessários durante o ciclo de vida da PGSI, assim como aplicar sanções e punições, quando necessário.

Além disso, as entidades compreendidas no escopo devem cumprir com os termos descritos, respondendo no caso do descumprimento com os mesmos, conforme capítulo a seguir.

4.3.1.6 SANÇÕES, PUNIÇÕES E CASOS OMISSOS

Neste capítulo explicitamos que qualquer violação ou tentativa de violação às políticas, normas e procedimentos são passíveis de penalidades, que incluem advertência verbal ou por escrito, suspensão e, em casos extremos, demissão por justa causa.

Além disso, definimos também a tratativa no caso de violações por terceiros e/ou que firam a legislação vigente e/ou que incorrem a danos à empresa.

Por último, esclarecemos a tratativa para casos não previstos nos documentos e recomendamos aos usuários a adoção de outras medidas de segurança além das previstas, de forma a garantir a proteção das informações da empresa.

4.3.1.7 GLOSSÁRIO

No glossário contextualizamos os principais termos técnicos utilizados na Política de Segurança da Informação, de forma a garantir o entendimento por quem os lê – dentre eles:

- Segurança da Informação;
- Confidencialidade, disponibilidade, integridade e autenticidade;
- Ameaça;
- Incidente de Segurança da Informação;
- Comitê Gestor de Segurança da Informação;
- Usuário da informação.

4.3.1.8 REVISÕES E GESTÃO DA POLÍTICA

Por último, definimos o período de revisão dos documentos e finalizamos o documento com a declaração de aprovação da alta diretoria.

Concluída a Política Geral de Segurança da Informação, partimos para a definição das normas complementares, seguindo a mesma estrutura do documento principal.

Dessa forma temos:

4.3.2. EQUIPAMENTOS COMPUTACIONAIS

As normas de equipamentos computacionais, encontrada nos apêndices B e C, estabeleceram o uso aceitável dos equipamentos computacionais da empresa por seus usuários autorizados, tendo como principais diretrizes:

- Utilizar os equipamentos disponibilizados exclusivamente para exercer suas atividades profissionais, sendo expressamente proibida a utilização para fins particulares;
- Manusear os equipamentos de propriedade da empresa com cuidado, visando preservar seu estado de funcionamento e conservação;
- Não realizar qualquer tipo de manutenção ou modificação nos equipamentos sem autorização prévia;
- Desligar os equipamentos no final do expediente ou antes de ausentar-se por um período prolongado, a menos que haja uma justificativa plausível em virtude de atividades de trabalho;
- Ativar o bloqueio de tela protegido por senha ao afastar-se do computador;
- No desligamento ou término da relação de trabalho, devolver os equipamentos disponibilizados em estado de conservação adequado.

Aqui já definimos também as diretrizes referentes ao uso seguro de dispositivos móveis, mídias de armazenamento removível e equipamentos particulares (que fica a critério da empresa e, quando permitido, deve seguir os níveis de segurança estabelecidos nesta e nas demais normas).

4.3.3. MONITORAMENTO

A norma de monitoramento (disposta no apêndice D), por sua vez, detalhou a fiscalização dos recursos computacionais e serviços disponibilizados pela empresa, tendo como objetivo evitar e identificar violações das condições da PGSI e da legislação vigente.

Aqui deixamos explícito que qualquer recurso computacional, serviço ou informação transitada na rede corporativa está sujeita a monitoramento, não havendo qualquer expectativa de privacidade na utilização dos mesmos.

4.3.4. EMAIL E COMUNICADORES INSTANTÂNEOS

Já a norma de email e comunicadores instantâneos estabeleceu a utilização segura desses serviços.

Ela pode ser encontrada no apêndice E e tem como principal objetivo proibir ações como:

- Utilizar dos serviços providos pela empresa para fins pessoais ou que não sejam de interesse da empresa;
- Enviar informações de uso interno ou confidencial para entidades fora do domínio corporativo da empresa, exceto quando expressamente autorizado;
- Forjar ou simular falsa identidade;
- Fazer o envio de mensagens indesejadas (spam) ou utilizar qualquer técnica que possa levar à sobrecarga dos serviços.

Além disso, aqui alertou-se também quanto à prática de phishing e ataques de engenharia social, muito comuns nesses serviços, descrevendo maneiras de identificar e evitar essas ameaças.

4.3.5. INTERNET E MÍDIAS SOCIAIS

A norma de internet e mídias sociais determinou o uso seguro e aceitável do acesso à internet e comportamento em mídias sociais por parte dos colaboradores.

A norma está disponível no apêndice F, proibindo:

• Qualquer espécie de conteúdo adulto, ato calunioso ou forma de preconceito, ameaça, chantagem ou assédio;

• A prática e/ou incitação de crimes;

• O desrespeito à imagem ou direitos de propriedade da empresa;

• A disseminação de códigos maliciosos ou ameaças virtuais;

• Qualquer tentativa de expor a infraestrutura da empresa a ameaças virtuais;

• A divulgação não autorizada de qualquer informação classificada como confidencial ou de uso interno de empresa;

• O uso de sites ou programas que contornem controles de acesso à internet;

• O uso da identidade visual ou a publicação de conteúdos diretamente relacionados à empresa e seus colaboradores sem autorização expressa.

4.3.6. CÓDIGOS MALICIOSOS

A norma de códigos maliciosos, localizada no apêndice G, instituiu os critérios a serem seguidos para proteger os recursos computacionais e informações de propriedade corporativa contra códigos maliciosos e ameaças virtuais.

Nela são detalhadas as ferramentas de proteção a serem utilizadas, assim como suas respectivas regras de uso.

Entretanto, mesmo com a existência delas, os usuários foram sugeridos também a adotar um padrão de comportamento seguro, de forma a reduzir a probabilidade de infecção e/ou a propagação de vírus como keyloggers, ransomware, adware e similares.

Para isso, definiu-se algumas regras, dentre elas:

• Não baixar arquivos recebidos de fontes suspeitas;

• Efetuar uma varredura antes de executar arquivos armazenados em mídias removíveis, baixados da internet ou recebidos por email ou comunicadores instantâneos;

• Não tentar efetuar o tratamento de códigos maliciosos por iniciativa própria;

• Não desenvolver, armazenar ou testar qualquer tipo de código malicioso;

• Reportar ao CGSI sobre qualquer ocorrência ou suspeita de infecção.

4.3.7. ACESSO REMOTO

Além das até então citadas, estabeleceu-se também uma norma para ditar o uso aceitável do acesso remoto aos usuários autorizados a essa modalidade, estando disposta no apêndice H.

Nela, descreveu-se os detalhes sobre a concessão do acesso e explicitou-se a responsabilidade do usuário sobre qualquer ação executada com suas credenciais (incluindo exercidas por terceiros não autorizados em posse delas, por exemplo), assim como definiu-se o nível mínimo de segurança dos equipamentos utilizados, que deve ser compatível com as normativas da empresa.

4.3.8. RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Já a norma de resposta a incidentes de Segurança da Informação, encontrada no apêndice I, estabeleceu as diretrizes necessárias para responder a eventos ou incidentes que impactaram, estejam impactando ou possam vir a impactar os recursos computacionais e/ou ativos de informação da empresa.

Aqui, ditou-se o que é entendido por incidente de segurança e o curso de ação a ser seguido para erradicá-los e restaurar os ativos afetados, assim como limitou-se a disseminação das informações sobre os incidentes a entidades externas sem a aprovação expressa do CGSI.

4.3.9. *BACKUP* E RESTAURAÇÃO DE DADOS

Por último, foi instaurada uma política de backup e restauração de dados (que já era seguida), a fim de documentar os critérios a serem seguidos nesse procedimento, para uso do técnico responsável.

Nela, buscou-se especificar de forma detalhada:

- O(s) responsável(is);
- A(s) ferramenta(s) a ser(em) utilizada(s);
- Os arquivos a serem resguardados;
- A frequência e o período de retenção das cópias, de acordo com o nível de criticidade dos dados;
- O tipo de backup (completo, incremental ou diferencial);
- O procedimento para verificação das cópias;
- A forma de armazenamento e, quando necessário, transporte das cópias;
- O procedimento para restauração dos dados resguardados;
- A forma de descarte das cópias antigas.

4.3.10. TERMO DE USO INTERNO

Criadas as normas complementares, foi expedido um termo de uso interno (localizado no apêndice J), formalizando a declaração do usuário com a compreensão e o comprometimento com as diretrizes estabelecidas na PGSI e em suas normas complementares.

Além disso, no termo o colaborador compromete-se também a não revelar informações de uso interno ou confidenciais relacionadas à empresa, mesmo após o encerramento do contrato de trabalho com a organização.

Sendo assim, a Política Geral de Segurança da Informação ficou estruturada da seguinte forma:

Tabela 2 – Estrutura da Política Geral de Segurança da Informação

Política Geral de Segurança da Informação	
Objetivos	• Estabelecer diretrizes e normas de Segurança da Informação • Definir os níveis de segurança a serem alcançados • Prevenir possíveis incidentes de segurança
Normas e procedimentos complementares	
Norma/procedimento	**Objetivo**
Ativos de informação e equipamentos computacionais	Definir o uso seguro dos ativos de propriedade da empresa
Internet e mídias sociais	Estabelecer o uso aceitável dos colaboradores nestes serviços
Serviços de e-mail e comunicadores instantâneos	
Códigos maliciosos	Instituir critérios e mecanismos de defesa para a proteção contra códigos maliciosos
Acesso remoto	Classificar o uso aceitável da modalidade de acesso remoto
Monitoramento	Detalhar a fiscalização dos recursos da empresa, a fim de garantir sua proteção
Resposta a incidentes	Definir o curso de ação a ser tomado no caso de um incidente
Backup e restauração de dados	Documentar os critérios a serem seguidos no processo de *backup* e restauração de dados
Termo de uso interno	
Objetivo	Formalizar o comprometimento do colaborador com as diretrizes dispostas

Fonte: elaborada pelo autor

4.4. ADEQUAÇÃO, APROVAÇÃO E DIVULGAÇÃO

Apresentada a primeira revisão da política ao diretor geral, juntamente às suas normas complementares, a mesma precisou passar por um processo de adaptação, a fim de adequá-las à realidade e às necessidades específicas da empresa.

Dentre as alterações, pode-se citar como as principais a redesignação de determinadas responsabilidades (que deixaram de ser do comitê como um todo e passaram e ser dos membros específicos [e vice-versa]) e a alteração ou remoção de cláusulas consideradas redundantes, com o objetivo de tornar a leitura por parte dos colaboradores menos maçante.

Posteriormente, o plano foi reapresentado à diretoria para poder então ser formalmente aprovado.

Após a aprovação das normas e diretrizes estabelecidas, promoveu-se uma campanha de divulgação, a fim de conscientizar os colaboradores quanto às normas implementadas, de forma a estabelecer um ambiente corporativo seguro.

Para tal, foi convocada uma conferência com a participação obrigatória de todos os funcionários da empresa, onde foram apresentados os principais pontos-chave da Política Geral de Segurança da Informação, assim como suas normas complementares.

Ao fim da reunião, foi entregue uma cópia da política a cada colaborador e dado um prazo de cinco dias úteis para a leitura dos documentos e aceite dos termos de uso pelos mesmos.

Além disso, também foram impressas e entregues aos colaboradores as cartilhas do CERT.br relevantes à política instituída, material que recomenda boas práticas em Segurança da Informação e alerta de forma descontraída e através de exemplos práticos sobre as principais ameaças encontradas no ambiente corporativo, assim como maneiras de identificá-las e evitá-las.

Figura 10 – Cartilha de boas práticas em redes sociais



Fonte: CERT.br, disponível em <https://cartilha.cert.br/fasciculos/redes-sociais/fasciculo-redes-sociais.pdf>

Dessa forma, a partir daqui, considera-se como implantado o Plano de Segurança da Informação.

4.5. AVALIAÇÃO

Passada a aprovação da Política Geral de Segurança da Informação na organização, o instrumento foi submetido a uma análise, feita por um Gestor de Tecnologia da Informação com cerca de 15 anos de experiência na área.

O profissional avaliou as diretrizes técnicas estabelecidas na política levando em consideração o porte e o *modus operandi* da empresa, tal como o levantamento feito previamente.

O avaliador aprovou a política, mas recomendou o estabelecimento de uma norma de classificação de informação (definindo os diferentes níveis de informação e suas respectivas formas de manuseio), assim como uma norma de gestão de identidade (especificando diretrizes quanto ao uso seguro de senhas e credenciais) em uma revisão futura do plano, o que não foi possível no presente estudo por conta da forma como a empresa é estruturada atualmente.

5. CONCLUSÕES

5.1. EM RELAÇÃO AO OBJETIVO GERAL

A implementação da Política de Segurança da Informação na empresa em questão materializou a Segurança da Informação no ambiente corporativo e possibilitou uma gestão de segurança eficaz, servindo como um recurso estratégico indispensável aos gestores da organização.

Entretanto, o desenvolvimento do plano demonstrou não ser tarefa fácil, principalmente por conta do capital humano restringido e dos recursos financeiros limitados, assim como pela falta de conhecimento dos colaboradores acerca do assunto.

Além disso, analisando o Plano de Segurança de grandes organizações, como a Unimed (exemplificada no fim do capítulo 2.3), UFSC, UDESC e o próprio IFSC (planos estes que também passaram por suas respectivas avaliações), nota-se que o instrumento proposto ao objeto de estudo desta pesquisa compartilha diversas similaridades com os citados e não deixa a desejar em nada – com exceção do corpo reduzido de agentes envolvidos na gestão do plano, devido ao porte da empresa.

Dessa forma, podemos considerar como bem sucedido o objetivo geral de desenvolvimento da Política de Segurança da Informação.

5.2. EM RELAÇÃO AOS OBJETIVOS ESPECÍFICOS

a) A análise bibliográfica acerca do assunto apontou que a Segurança da Informação é uma área altamente complexa, demonstrando a importância das organizações estabelecerem estratégias para se protegerem e possibilitando a identificação das principais ameaças de segurança, assim como seus respectivos mecanismos de defesa;

b) Já a identificação das atividades do Plano de Segurança da Informação, também através de pesquisa bibliográfica, possibilitou o descobrimento de uma estrutura internacionalmente aceita e, posteriormente, o aperfeiçoamento do plano;

c) A elaboração da política, por sua parte, formalizou as diretrizes de Segurança da Informação, proporcionando uma gestão de segurança corporativa eficaz à organização;

d) Por último, a avaliação do instrumento por um especialista auxiliou a identificação de pontos de fragilidade através de um ponto de vista externo, permitindo um aprimoramento ainda maior do mesmo.

5.3. TRABALHOS FUTUROS

Como recomendação de trabalhos futuros, fica como sugestão a implementação da Política de Segurança da Informação em outras organizações, tal como sua revisão, de forma a diminuir o número de ataques e vazamentos neste segmento.

Para tal, além do roteiro que foi seguido, considera-se como imprescindível as seguintes observações:

- Obter o apoio da alta direção;
- Alinhar a política à cultura corporativa da organização, não deixando de considerar também a cultura brasileira (empresas familiares, relações sociais flexíveis, pouco formalismo, “jeitinho brasileiro”, etc);
- Garantir a publicação das normas, assim como a compreensão e o aceite dos termos de uso por parte dos colaboradores;
- Sustentar a melhoria contínua do plano, afirmando a proteção dos ativos frente às novas ameaças que surgem todos os dias.

Além disso, recomenda-se também uma análise de viabilidade, assim como uma análise de vulnerabilidades de segurança, preferencialmente terceirizada.

Por último, sugere-se um acompanhamento mais longo dos resultados, tal como uma avaliação dos mesmos através de métricas, o que não foi possível na presente pesquisa por conta do tempo de execução da mesma.

REFERÊNCIAS

ADACHI, Tomi. **Gestão de segurança em internet banking**: estudo de casos brasileiros. 2004. 121 f. Dissertação (Mestrado) - Curso de Administração de Empresas, Escola de Administração de Empresas de São Paulo, São Paulo, 2004. Disponível em: <https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/2339/67929.pdf>. Acesso em: 04 nov. 2022.

ANDERSON, R. **Security Officer-1**: guia oficial para formação de gestores em segurança da informação. Porto Alegre: Zouk, 2006.

ARAÚJO, Márcio Tadeu de; FERREIRA, Fernando Nicolau Freitas. **Política de Segurança da Informação**: Guia Prático para Elaboração e Implementação. Rio de Janeiro: Ciência Moderna, 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799**: Tecnologia da informação - Código de prática para a gestão da segurança da informação. 1. ed. Rio de Janeiro: ABNT, 2001.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001**: Tecnologia da informação – Técnicas de segurança – Sistema de gestão de segurança da informação – Requisitos. 1. ed. Rio de Janeiro: ABNT, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. 1. ed. Rio de Janeiro: ABNT, 2005.

BEAL, Adriana. **Segurança da Informação**: Princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005. 175 p.

BEZERRA, Anne Caroline Dias. **UMA MODELAGEM DE SEGURANÇA DA INFORMAÇÃO BASEADA NA ISO/IEC 27001 E GESTÃO ITIL APLICADA ÀS MICROS E PEQUENAS EMPRESAS**. 2015. 88 f. TCC (Graduação) - Curso de Tecnologias da Informação e Comunicação, Universidade Federal de Santa Catarina, Araranguá, 2015. Disponível em: <https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/133709/Anne_tcc_201501.pdf>. Acesso em: 04 nov. 2022.

BOGDAN, Roberto C.; BIKLEN, Sari Knopp. **Investigação qualitativa em educação**. Tradução Maria João Alvarez, Sara Bahia dos Santos e Telmo Mourinho Baptista. Porto: Porto Editora, 1994.

CASTRO, Rogério Artiaga de Almeida. **SEGURANÇA E GARANTIA DA INFORMAÇÃO**: um estudo de caso em organização pública. 2010. 73 f. Dissertação (Mestrado) - Curso de Gestão do Conhecimento e Tecnologia da Informação, Universidade Católica de Brasília, Brasília, 2010. Disponível em: <https://bdtd.ucb.br:8443/jspui/bitstream/123456789/1357/1/Rogerio%20Artiaga%20de%20Almeida%20Castro.pdf>. Acesso em: 04 nov. 2022.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL, CERT.BR. **Cartilha de Segurança para Internet**. 2. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012. 140 p.

DINAMIO. **Tipos de ataques de enganação e como se previnir**. Disponível em: <https://www.dinamio.com.br/blog/2020/12/07/tipos-de-ataques-de-enganacao-e-como-se-prevenir/>. Acesso em: 04 nov. 2022.

DODT, Cláudio. **ISO 27001**: Construindo Políticas de Segurança da Informação. Disponível em: <https://www.udemy.com/course/politicasegurancainformacao>. Acesso em: 25 out. 2022.

FERREIRA, Fernando Nicolau Freitas. **Segurança da Informação**. Rio de Janeiro: Ciência Moderna, 2003. 162 p.

FONTES, Edison Luiz Gonçalves. **Praticando a Segurança da Informação**. Rio de Janeiro: Brasport, 2008.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4ª. ed. São Paulo: Atlas S/A, 2002.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. Tradução Maria Lúcia Blanck Lisbôa. Porto Alegre: Bookman, 2013. 550 p.

HORI, Andre Shigueru. **Modelo de Gestão de Risco em Segurança da Informação**: um estudo de caso no mercado brasileiro de cartões de crédito. 2003. 204 f. Dissertação (Mestrado) - Curso de Administração, Escola de Administração de Empresas de São Paulo, São Paulo, 2003. Disponível em: <https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/2216/74539.pdf>. Acesso em: 04 nov. 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27000**: Information technology - Security techniques - Information security management systems - Overview and vocabulary. 1. ed. Genebra: 2016.

KEEN, P. G. W. **Guia gerencial para a tecnologia da informação**: conceitos essenciais e terminologia para empresas e gerentes. Rio de Janeiro: Campus, 1996.

LYRA, Maurício R. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro: Ciência Moderna, 2008.

MITNICK, Kevin D.; SIMON, William L.. **MITNICK – A Arte de Enganar**: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. Tradução Kátia Aparecida Roque. São Paulo: Pearson Education do Brasil, 2003. 284 p.

MORAES, Alexandre Fernandes de. **Segurança em Redes**: fundamentos. 1. ed. São Paulo: Érica, 2010. 262 p.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de Redes em Ambientes Corporativos**. São Paulo: Novatec, 2007. 488 p.

PRESSMAN, Roger S. **Engenharia de Software**. Mc Graw Hill, 6 ed, Porto Alegre, 2010.

SÊMOLA, M. **Gestão da Segurança da Informação** - Uma visão executiva. Rio de Janeiro: Campus, 2003. 156 p.

SÊMOLA, M. **Gestão da Segurança da Informação** - Uma visão executiva - 2 ed. São Paulo: Elsevier, 2014.

SONICWALL. **Relatório De Ameaças Cibernéticas Da Sonicwall 2022**. Disponível em: <https://www.sonicwall.com/pt-br/2022-cyber-threat-report/>. Acesso em: 04 nov. 2022.

STATISTA. **Average duration of downtime after a ransomware attack from 1st quarter 2020 to 4th quarter 2021**. Disponível em: <https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/>. Acesso em: 04 nov. 2022.

UNIMED. **POLÍTICA DE SEGURANÇA E PRIVACIDADE DA INFORMAÇÃO**. Disponível em: <https://www.unimed.coop.br/site/documents/1221729/7749667/POL-TI-001.r07_POLITICA_DE_SEGURANCA_E_PRIVACIDADE_DA_INFORMACAO.pdf/>. Acesso em: 05 nov. 2022.

YIN, Robert K. **Estudo de caso**: planejamento e métodos. Porto Alegre: Bookman, 2005.

APÊNDICE A – POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

1. Introdução

1.1. A EMPRESA tem como missão trazer ao mercado ferramentas com alto valor agregado, de fácil utilização, inovadoras e essenciais à organização empresarial;

1.2. A EMPRESA entende que a informação corporativa é um bem essencial para suas atividades e compreende que a manipulação de sua informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer sua segurança;

1.3. Dessa forma, a EMPRESA estabelece sua Política Geral de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada às boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações da organização ou sob sua responsabilidade.

2. Propósito

2.1. Esta política tem por propósito estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores adotar padrões de comportamento seguro;

2.2. Resguardar suas informações através da garantia dos requisitos básicos de confidencialidade, integridade e disponibilidade;

2.3. Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus empregados, clientes e parceiros, minimizando o risco de perdas financeiras, participação de mercado, confiança de clientes ou qualquer outro impacto negativo no negócio da empresa.

3. Escopo

3.1. Esta política se aplica a todos os usuários da informação da EMPRESA, incluindo qualquer indivíduo ou organização que possui vínculo com a empresa, tais como empregados, prestadores de serviço e colaboradores que possuem acesso às informações da empresa e/ou fazem uso dos recursos computacionais compreendidos em sua infraestrutura.

4. Diretrizes

4.1. A Diretoria Executiva e o Comitê Gestor de Segurança da Informação estão comprometidos com uma gestão efetiva de Segurança da Informação na EMPRESA. Desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às necessidades da organização.

4.2. Sendo assim, é política da EMPRESA:

4.2.1. Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação sejam atingidos;

4.2.2. Disponibilizá-las a todas as partes interessadas e autorizadas e garantir sua conscientização e educação, promovendo uma cultura de segurança corporativa;

4.2.3. Atender integralmente aos requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;

4.2.4. Tratar integralmente incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicados às autoridades apropriadas;

4.2.5. Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres.

5. Papéis e Responsabilidades

5.1. COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO - CGSI

5.1.1. Fica constituído o COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO, contando com a participação do diretor geral e de, pelo menos, um membro sênior das seguintes áreas: Tecnologia da Informação, Segurança da Informação, Recursos Humanos, Jurídico e Comunicação.

5.1.2. É responsabilidade do CGSI:

5.1.2.1. Analisar, revisar e propor a aprovação de políticas e normas relacionadas à Segurança da Informação;

5.1.2.2. Garantir a disponibilidade dos recursos necessários para uma gestão efetiva, em conformidade com esta política e suas demais resoluções;

5.1.2.3. Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;

5.1.2.4. Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.

5.1.2.5. Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados;

5.1.2.6. Revisá-las periodicamente, ajustando a classificação e rotulagem das mesmas conforme necessário;

5.1.2.7. Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

5.1.2.8. Tomar as ações cabíveis para se fazer cumprir os termos desta política.

5.2. USUÁRIOS DA INFORMAÇÃO

5.2.1. É responsabilidade dos Usuários da Informação:

5.2.1.1. Ler, compreender e cumprir integralmente os termos da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;

5.2.1.2. Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Segurança da Informação, suas normas e procedimentos ao comitê;

5.2.1.3. Reportar qualquer evento que viole esta política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais corporativos;

5.2.1.4. Assinar o Termo de Uso de Sistemas de Informação, formalizando a ciência e o aceite integral das disposições da presente política, bem como suas demais normas e procedimentos, assumindo responsabilidade pelo seu cumprimento;

5.2.1.5. Responder pela inobservância das mesmas, conforme definido no item sanções e punições.

6. Sanções e Punições

6.1. As violações ou tentativas de violação desta política, bem como suas demais normas e procedimentos, serão passíveis de penalidades, que incluem advertência verbal ou por escrito, suspensão não remunerada e, em caso extremos, demissão por justa causa;

6.2. A aplicação de sanções e punições será realizada conforme a análise do Comitê Gestor de Segurança da Informação, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o CGSI, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave;

6.3. No caso de terceiros contratados ou prestadores de serviço, o comitê deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato;

6.4. Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano à empresa, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nos itens 6.1, 6.2 e 6.3 desta política.

7. Casos Omissos

7.1. Os casos omissos serão avaliados pelo Comitê Gestor de Segurança da Informação para posterior deliberação;

7.2. As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações da empresa.

8. Glossário

8.1. Segurança da informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da empresa;

8.2. Confidencialidade: Propriedade dos ativos da informação de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas;

8.3. Disponibilidade: Propriedade dos ativos da informação de serem acessíveis e utilizáveis sob demanda, por partes autorizadas;

8.4. Integridade: Propriedade dos ativos da informação de serem exatos e completos;

8.5. Ativo de informação: Patrimônio intangível da EMPRESA, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro ou mercadológico, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição ou confiadas à empresa por parceiros, clientes, empregados e terceiros, independente do formato de trafegação ou armazenamento;

8.6. Ameaça: Causa potencial de um incidente, que pode vir a prejudicar a empresa;

8.7. COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO – CGSI: Grupo de trabalho efetivado pela diretoria, responsável por tratar questões ligadas à Segurança da Informação;

8.8. Incidente de segurança da informação: Um evento ou conjunto de eventos indesejados que tem possibilidade significativa de afetar as operações ou ameaçar as informações da empresa;

8.9. Usuário da informação: Empregados com vínculo empregatício de qualquer área ou terceiros alocados na prestação de serviços à empresa, assim como outros indivíduos ou organizações devidamente autorizados a utilizar qualquer ativo de informação da EMPRESA para o desempenho de suas atividades profissionais.

9. Revisões

9.1. Esta política é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

10. Gestão da Política

10.1. A Política Geral de Segurança da Informação foi aprovada pelo Comitê Gestor de Segurança da Informação em conjunto com a diretoria no dia 17/10/2022.

APÊNDICE B – NORMA DE ATIVOS DE INFORMAÇÃO

1. Introdução

1.1. A presente norma complementa a Política Geral de Segurança da Informação, definindo as diretrizes para o uso aceitável de ativos de informação da EMPRESA.

2. Propósito

2.1. Estabelecer diretrizes para o uso aceitável, entendido como seguro, dos ativos de informação da empresa por seus usuários autorizados.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. Uso de equipamento computacional

4.1.1. A EMPRESA fornece a seus usuários equipamentos para o desempenho exclusivo de suas atividades profissionais;

4.1.2. Sendo assim, os usuários devem observar as seguintes disposições quanto ao uso de equipamentos de propriedade da EMPRESA:

4.1.2.1. Os equipamentos são disponibilizados com o objetivo específico de permitir aos usuários desenvolverem suas atividades profissionais, sendo expressamente proibida a utilização para fins particulares;

4.1.2.2. A alteração e/ou a manutenção de qualquer equipamento de propriedade da EMPRESA é uma atribuição específica do departamento de Tecnologia da Informação que, a seu critério exclusivo, poderá delegar formalmente outro responsável. Sendo assim, demais usuários são expressamente proibidos de realizar qualquer tipo de manutenção ou modificação nos equipamentos;

4.1.2.3. Os equipamentos disponibilizados devem ser utilizados com cuidado, visando garantir sua preservação e seu funcionamento adequado;

4.1.2.4. Computadores de mesa (*desktops*) ou móveis (*notebooks*) devem ser desligados no final do expediente ou sempre que um usuário estiver ausente por um período prolongado, excetuando-se quando existir uma justificativa plausível em virtude de atividades de trabalho;

4.1.2.5. O bloqueio de tela protegido por senha deverá ser ativado sempre que o usuário se afastar do computador de mesa ou móvel que esteja utilizando;

4.1.2.6. Ao final do contrato de trabalho, os equipamentos disponibilizados devem ser devolvidos em estado de conservação adequado quando no desligamento ou término da relação do usuário com a empresa;

4.1.2.7. Qualquer dano aos equipamentos fornecidos será devidamente analisado pela área de Tecnologia da Informação. Havendo a constatação de que tal dano decorreu de ação direta ou omissão do usuário, caberá à empresa exercer seu direito de reparação ao prejuízo, através da tomada das medidas cabíveis.

4.1.3. A seu critério exclusivo, a empresa poderá permitir a utilização de equipamento particular para o desempenho de atividades profissionais, devendo os mesmos passar por inspeção tanto do departamento de Tecnologia da Informação, quanto da área de Segurança da Informação, de forma a garantir a adequação aos requisitos e controles de segurança adotados pela empresa;

4.1.4. Não é permitida a conexão de equipamentos particulares na rede corporativa sem autorização prévia.

4.2. Dispositivos de Armazenamento Removível

4.2.1. A empresa poderá, a seu critério exclusivo, fornecer a seus usuários dispositivos móveis ou com capacidade de armazenamento removível para execução de atividades profissionais, devendo ser observadas, além das diretrizes acima, as seguintes:

4.2.1.1. O usuário é o responsável direto pela segurança física e lógica dos dispositivos móveis sob sua guarda. Portanto, os mesmos não devem permanecer fora de seu alcance em locais públicos ou onde haja o acesso não controlado de pessoas;

4.2.1.2. Durante o deslocamento, o usuário deve permanecer alerta e manter uma conduta discreta, dando preferência a compartimentos de armazenamento resistentes e não chamativos e nunca deixando o dispositivo móvel desacompanhado;

4.2.1.3. A instalação de ferramentas de proteção para dispositivos móveis é realizada pelo departamento de Tecnologia da Informação, sendo obrigatória para todos os equipamentos corporativos;

4.2.1.4. Em caso de perda ou furto de um dispositivo de armazenamento removível, o usuário deve comunicar imediatamente o departamento de segurança patrimonial para que possam ser tomadas as medidas cabíveis.

4.3. Armazenamento remoto (nuvem)

4.3.1. A empresa disponibiliza a seus usuários espaço para armazenamento remoto de arquivos na nuvem, através de sua solução corporativa;

4.3.2. Não é permitido o uso de qualquer outra solução além da oficialmente adotada e homologada pela empresa.

4.4. Identificação digital

4.4.1. A empresa poderá, a seu critério exclusivo, fornecer certificados digitais para a execução de atividades profissionais específicas, devendo ser observadas as seguintes diretrizes:

4.4.1.1. Cabe exclusivamente ao usuário a conservação de seu certificado digital, independentemente do equipamento que o suporte, bem como de qualquer tipo de senha ou meio de autenticação relacionado ao mesmo.

4.4.1.2. O usuário deverá informar à equipe de Segurança da Informação sobre qualquer evento ou suspeita relativa ao comprometimento de sua senha e/ou o uso indevido de seu certificado digital;

4.4.1.3. O usuário desligado ou em processo de desligamento terá o certificado digital expedido pela empresa imediatamente revogado;

4.5. Equipamentos de impressão e reprografia

4.5.1. O uso de equipamentos de impressão e reprografia (fotocopiadoras) deve ser feito exclusivamente para a impressão/reprodução de documentos que sejam de interesse da empresa e/ou que estejam relacionados com o desempenho das atividades profissionais do usuário.

4.5.2. Na utilização destes equipamentos, o usuário deve observar as seguintes disposições:

4.5.2.1. O usuário deve retirar imediatamente da impressora ou fotocopiadora os documentos que tenha solicitado a impressão, transmissão ou cópia que contenham informações classificadas como de uso interno ou confidencial;

4.5.2.2. A impressão ou cópia de documento em suporte físico deve ser limitada à quantidade exata necessária para a tarefa determinada;

4.5.2.3. Não será admissível o reaproveitamento de páginas já impressas e contendo informações classificadas como confidenciais, devendo as mesmas ser descartadas de acordo com os procedimentos adotados pela empresa.

4.6. Segurança física

4.6.1. As instalações de processamento das informações da EMPRESA serão mantidas em áreas seguras, cujo perímetro é fisicamente isolado contra o acesso não autorizado, os danos e quaisquer interferências de origem humana ou natural.

4.6.2. O usuário deve observar as seguintes disposições específicas quanto à segurança física:

4.6.2.1. Excetuando-se quando formalmente autorizado, terceiros nunca devem ser deixados sozinhos em áreas sensíveis;

4.6.2.2. É resguardado à empresa o direito de inspecionar malas, maletas, mochilas e similares, assim como quaisquer equipamentos, incluindo dispositivos móveis, antes de permitir a entrada ou saída de colaboradores ou terceiros de áreas sensíveis;

4.6.2.3. É resguardado também o direito de monitorar seus ambientes físicos, através do circuito interno de câmeras em áreas comuns. As imagens obtidas serão armazenadas e protegidas contra qualquer tipo de manipulação indevida;

4.6.2.4. Os documentos classificados como internos ou confidenciais, após manuseados, não deverão ser deixados expostos, cabendo ao usuário o dever de mantê-los guardados ou descartá-los de acordo com os procedimentos determinados pela organização;

4.6.2.5. Não é permitido o consumo de qualquer tipo de alimento, bebida ou fumo em áreas apontadas como sensíveis.

5. Papéis e Responsabilidades

5.1. GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO

5.1.1. É responsabilidade da Gerência de Segurança da Informação:

5.1.1.1. Estabelecer e manter atualizados os procedimentos complementares a esta norma;

5.1.1.2. Tratar eventuais tentativas, bem sucedidas ou não, de desvio de conduta dos termos dessa norma.

6. Sanções e Punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma N-SI-001 foi aprovada pelo Comitê Gestor de Segurança da Informação em conjunto com a diretoria no dia 17/10/2022.

APÊNDICE C – NORMA DE USO DE EQUIPAMENTOS COMPUTACIONAIS PESSOAIS

1. Introdução

1.1. A presente norma complementa a Política Geral de Segurança da Informação, definindo as diretrizes para utilização segura de dispositivos computacionais pessoais.

2. Propósito

2.1. Estabelecer diretrizes para utilização segura de dispositivos computacionais pessoais no ambiente corporativo da EMPRESA ou para o manuseio de suas informações.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. Uso de equipamentos computacionais pessoais no ambiente corporativo

4.1.1. A empresa fornece todos os recursos computacionais necessários para que seus colaboradores executem suas atividades laborais;

4.1.2. Entretanto, a seu critério exclusivo, a empresa poderá permitir o uso de dispositivos particulares para a execução de atividades profissionais ou o manuseio de informações de sua propriedade;

4.1.3. A permissão para destes dispositivos é prerrogativa da diretoria, devendo o usuário estar formalmente autorizado e concordar integralmente com os termos desta norma antes de fazer o uso dos mesmos;

4.1.4. O uso não autorizado de qualquer dispositivo particular no ambiente corporativo será considerado uma violação da política e tratado como um incidente de Segurança da Informação, estando o responsável sujeito às sanções e punições previstas neste instrumento;

4.1.5. A empresa não será responsável por fornecer o suporte, atualização, manutenção, reposição, licenciamento, reembolso ou cobrir qualquer tipo de custo referente ao uso de dispositivos particulares;

4.1.6. O uso de dispositivos particulares não modifica a propriedade da organização sobre as informações, permanecendo qualquer direito de propriedade intelectual com a empresa;

4.1.7. Quando autorizados, os usuários serão inteiramente responsáveis por garantir a segurança de seus dispositivos, garantindo que:

4.1.7.1. O sistema operacional dos dispositivos estará sempre atualizado e com todas as correções de segurança aplicadas;

4.1.7.2. Os dispositivos possuam ferramenta para prevenção de códigos maliciosos alinhada com os padrões de segurança adotados pela organização;

4.1.7.3. Os dispositivos utilizem apenas softwares licenciados, preservando o direito autoral.

5. Papéis e Responsabilidades

5.1. COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO

5.1.1. É responsabilidade do comitê:

5.1.1.1. Avaliar, aprovar ou negar solicitações para uso de dispositivos particulares no ambiente corporativo.

6. Sanções e Punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma N-SI-002 foi aprovada pelo Comitê Gestor de Segurança da Informação em conjunto com a diretoria da empresa no dia 17/10/2022.

APÊNDICE D – NORMA DE MONITORAMENTO

1. Introdução

1.1. A presente norma complementa a Política Geral de Segurança da Informação, definindo as diretrizes para o monitoramento de ativos, serviços e recursos computacionais da EMPRESA.

2. Propósito

2.1. Estabelecer diretrizes para o monitoramento de ativos, serviços de informação e recursos computacionais da empresa, garantindo o respeito dos usuários às regras estabelecidas na Política Geral de Segurança da Informação, bem como produzir prova de eventual violação das condições constantes da mesma e na legislação vigente.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. Monitoramento de ativos/serviços da informação e recursos computacionais

4.1.1. Qualquer ativo, serviço de informação ou recurso computacional da empresa, bem como seu ambiente físico e qualquer outro dispositivo com acesso aos mesmos, estão sujeitos a monitoramento, visando exclusivamente resguardar a segurança dos ativos de informação e segurança jurídica da empresa, não constituindo qualquer violação à intimidade, vida privada, honra ou imagem da pessoa monitorada;

4.1.2. Sendo assim, não há qualquer expectativa de privacidade na utilização dos ativos, serviços de informação ou recursos computacionais da empresa, incluindo o serviço de email corporativo, comunicadores instantâneos e navegação em sites da internet através da infraestrutura corporativa;

4.1.3. Todas as informações dos ativos, serviços de informação ou recursos computacionais corporativos, incluindo dados sensíveis e/ou criptografados, podem ser interceptadas, gravadas, lidas, copiadas e divulgadas por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais.

4.2. Monitoramento do ambiente físico

4.2.1. A EMPRESA faz o monitoramento do seu ambiente físico através do uso de circuito interno de câmeras instaladas em suas dependências, tendo como objetivo assegurar sua segurança patrimonial;

4.2.2. As imagens captadas dentro das dependências da empresa serão arquivadas conforme procedimento adotado pela instituição e mantidas em caráter estritamente confidencial, somente podendo ser divulgadas em caso de infração às regras constantes em suas políticas e normas e/ou infração de legislação vigente;

4.2.3. Não é permitido o uso de qualquer dispositivo de gravação audiovisual dentro do perímetro físico da empresa, excetuando-se quando o usuário estiver formalmente autorizado.

5. Papéis e Responsabilidades

5.1. COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO

5.1.1. É responsabilidade do COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO:

5.1.1.1. Realizar o monitoramento dos ativos, serviços de informação e recursos computacionais corporativos;

5.1.1.2. Tratar eventuais violações das diretrizes de segurança identificadas através de ferramentas de monitoramento.

6. Sanções e Punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma N-SI-003 foi aprovada pelo Comitê Gestor de Segurança da Informação em conjunto com a diretoria no dia 17/10/2022.

APÊNDICE E – NORMA DE COMPORTAMENTO EM SERVIÇOS DE EMAIL E COMUNICADORES INSTANTÂNEOS

1. Introdução

1.1. A presente norma complementa a Política Geral de Segurança da Informação, definindo as diretrizes para utilização dos serviços de email e comunicadores instantâneos.

2. Propósito

2.1. Estabelecer diretrizes para utilização segura dos serviços de email e comunicadores instantâneos fornecidos pela EMPRESA.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. Serviços de e-mail e comunicadores instantâneos

4.1.1. A EMPRESA fornece os serviços de email e comunicadores instantâneos para seus usuários autorizados, exclusivamente para o desempenho de suas atividades profissionais;

4.1.2. Não é permitido o uso de qualquer serviço de email além do oficialmente fornecido;

4.1.3. Durante o uso desses serviços, não é permitido:

4.1.3.1. Utilizá-los em caráter pessoal ou para fins que não sejam de interesse da empresa;

4.1.3.2. Utilizar de termos ou palavras de baixo calão na redação de mensagens;

4.1.3.3. Enviar informação classificada como de uso interno ou confidencial para endereços eletrônicos que não fazem parte do domínio corporativo da empresa, excetuando-se quando expressamente autorizados;

4.1.3.4. Inscrever qualquer endereço de email da empresa em listas de distribuição ou grupos de discussão que não estejam relacionadas com atividades laborais ou do interesse da organização;

4.1.3.5. Fazer uso de qualquer técnica de falsificação ou simulação de falsa identidade;

4.1.3.6. Tentar a interceptação ou alteração do conteúdo da mensagem de outros usuários;

4.1.3.7. Utilizar dos serviços para o envio de mensagens indesejadas (spam) ou qualquer tipo de técnica que possa levar a sobrecarga do serviço;

4.1.3.8. Usar dos serviços para disseminar ou transmitir mensagens de caráter injurioso, calunioso ou que possam ferir a legislação em vigor.

4.2. Monitoramento

4.2.1. Os serviços de email corporativo e comunicadores instantâneos são continuamente monitorados, com o objetivo de proteger a organização e atestar o respeito às regras estabelecidas, bem como produzir evidências relativas à eventual violação das mesmas e/ou à legislação em vigor. Sendo assim, não há qualquer tipo de expectativa de privacidade por parte dos usuários;

4.2.2. Durante o monitoramento, a empresa se resguarda o direito de, sem qualquer notificação ou aviso, de monitorar, interceptar, registrar, ler, bloquear, redirecionar, retransmitir, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais todas as mensagens enviadas ou recebidas pelos usuários através de seu serviço de email.

5. Papéis e Responsabilidades

5.1. GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

5.1.1. É responsabilidade da gerência de tecnologia da informação:

5.1.1.1. Controlar e monitorar os serviços de email e comunicadores instantâneos fornecidos pela EMPRESA.

6. Sanções e Punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma N-SI-004 foi aprovada pelo Comitê Gestor de Segurança da Informação em conjunto com a diretoria no dia 17/10/2022.

APÊNDICE F – NORMA DE COMPORTAMENTO NA INTERNET E MÍDIAS SOCIAIS

1. Introdução

1.1. A presente norma complementa a Política Geral de Segurança da Informação, definindo as diretrizes para utilização segura do acesso à internet e comportamento em mídias sociais.

2. Propósito

2.1. Estabelecer diretrizes para utilização segura do acesso à internet fornecido pela EMPRESA e do comportamento de colaboradores em mídias e redes sociais.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. Acesso à internet

4.1.1. A EMPRESA fornece acesso à internet aos seus usuários autorizados, conforme as necessidades inerentes ao desempenho de suas atividades profissionais;

4.1.2. O acesso à internet pode ser fornecido tanto através da rede corporativa quanto através da disponibilização de serviços de internet móvel contratados;

4.1.3. Toda informação acessada, transmitida, recebida ou produzida através do acesso à internet fornecido pela empresa está sujeita a monitoramento, não havendo por parte do usuário qualquer expectativa de privacidade;

4.1.4. Durante o monitoramento do acesso à internet, a empresa se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, ler, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais, qualquer informação trafegada por sua rede;

4.1.5. Durante o acesso à internet fornecido pela empresa, não é permitido o download, o upload, a visualização ou o armazenamento de qualquer conteúdo relacionado direta ou indiretamente com:

4.1.5.1. Qualquer espécie de conteúdo adulto;

4.1.5.2. Qualquer forma de ameaça, chantagem e assédio moral ou sexual;

4.1.5.3. Qualquer ato calunioso, difamatório, infamante, vexatório, aviltante ou atentatório à moral e aos bons costumes da sociedade;

4.1.5.4. Qualquer forma de preconceito baseado em cor, raça, sexo, gênero, origem, condição social, crença, religião, deficiências e necessidades especiais;

4.1.5.5. A prática e/ou a incitação de crimes ou contravenções penais;

4.1.5.6. A prática de propaganda política nacional ou internacional;

4.1.5.7. A prática de quaisquer atividades comerciais desleais;

4.1.5.8. O desrespeito à imagem ou aos direitos de propriedade intelectual da empresa;

4.1.5.9. A disseminação de códigos maliciosos e ameaças virtuais;

4.1.5.10. Tentativa de expor a infraestrutura computacional da empresa a ameaças virtuais;

4.1.5.11. A divulgação não autorizada de qualquer informação corporativa classificada como confidencial ou de uso interno;

4.1.5.12. O uso de sites ou serviços que busquem contornar controles de acesso à internet.

4.2. Comportamento corporativo em mídias e redes sociais

4.2.1. A publicação de conteúdo referente à EMPRESA em mídias e redes sociais é feita por setores e usuários que possuem essa responsabilidade específica, sendo os demais usuários proibidos de publicar qualquer tipo de informação em nome da organização;

4.2.2. Quando no uso de suas mídias e redes sociais particulares, os colaboradores devem observar as seguintes restrições:

4.2.2.1. Não é permitido o uso de qualquer parte da identidade visual da EMPRESA sem autorização prévia e expressa;

4.2.2.2. Não é permitida a publicação de conteúdos ou comentários diretamente relacionados à empresa ou aos seus colaboradores;

4.2.2.3. Não é permitida a publicação de qualquer tipo de imagem, foto, vídeo, áudio relacionado ao ambiente corporativo da empresa sem a expressa autorização da organização, excetuando-se material divulgado em canais oficiais.

5. Papéis e Responsabilidades

5.1. GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

5.1.1. É responsabilidade da gerência de tecnologia da informação:

5.1.1.1. Controlar e monitorar qualquer tipo de acesso à internet fornecido pela EMPRESA.

6. Sanções e Punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma N-SI-005 foi aprovada pelo Comitê Gestor de Segurança da Informação em conjunto com a diretoria no dia 17/10/2022.

APÊNDICE G – NORMA DE CÓDIGOS MALICIOSOS

1. Introdução

1.1. A presente norma complementa a Política Geral de Segurança da Informação, definindo as diretrizes para proteção contra ameaças e códigos maliciosos de qualquer natureza.

2. Propósito

2.1. Estabelecer diretrizes para a proteção dos ativos e serviços de informação da EMPRESA contra ameaças e códigos maliciosos de qualquer natureza.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. Ferramenta de proteção contra códigos maliciosos

4.1.1. A EMPRESA disponibiliza ferramentas para proteção dos seus ativos e serviços de informação e recursos computacionais, incluindo estações de usuários, dispositivos móveis e servidores corporativos, contra ameaças e códigos maliciosos tais como cavalos de tróia, ferramentas de captura de tela e dados digitados, adware, ransomware e similares;

4.1.2. Apenas a ferramenta disponibilizada pela EMPRESA deve ser utilizada na proteção contra códigos maliciosos;

4.1.3. A ferramenta de proteção contra códigos maliciosos da EMPRESA adota as seguintes regras de uso:

4.1.3.1. Atualização em tempo real do arquivo de assinaturas de códigos maliciosos e varredura diária em estações de usuários e servidores corporativos;

4.1.3.2. As varreduras diárias devem analisar todos os arquivos em cada uma das unidades de armazenamento locais das estações de usuários e dispositivos móveis;

4.1.3.3. As varreduras diárias em servidores corporativos podem ser limitadas a pastas ou arquivos específicos, de modo a evitar o comprometimento do desempenho de recursos computacionais críticos;

4.1.3.4. As funções de proteção em tempo real e detecção com base no comportamento devem estar habilitadas para todas as estações de usuários e dispositivos móveis;

4.1.3.5. Sites, serviços e arquivos baixados da internet detectados como possíveis ameaças serão automaticamente bloqueados em estações de usuários, dispositivos móveis e servidores corporativos;

4.1.4. Em caso de ocorrência ou suspeita de infecção em uma estação ou dispositivo móvel, a mesma deverá ser imediatamente isolada da rede corporativa e de qualquer comunicação com a internet;

4.1.5. Em caso de ocorrência ou suspeita de infecção no servidor, deverão ser adotadas medidas para garantir o isolamento do mesmo da rede corporativa e da internet, levando em consideração o impacto da desativação dos serviços publicados no referido servidor;

4.2. Prevenção dos usuários contra códigos maliciosos

4.2.1. Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os usuários devem adotar um comportamento seguro, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos através das seguintes regras:

4.2.1.1. Não tentar efetuar o tratamento ou correção de códigos maliciosos por conta própria;

4.2.1.2. Reportar imediatamente ao Comitê Gestor sobre qualquer infecção ou suspeita de infecção;
4.2.1.3. Não desenvolver, testar ou armazenar qualquer tipo de código malicioso;
4.2.1.4. Efetuar uma varredura com a ferramenta de proteção contra códigos maliciosos fornecida antes de utilizar arquivos armazenados em mídias removíveis, baixados da internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos;
4.2.1.5. Não executar arquivos recebidos ou baixados de fontes suspeitas. Caso necessário, poderá ser solicitado o apoio da equipe de Segurança da Informação para validar se o arquivo representa ou não uma ameaça.

5. Papéis e Responsabilidades

5.1. GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

5.1.1. É responsabilidade da gerência de tecnologia da informação:
5.1.1.1. Tratar casos de infecção ou suspeita de infecção por códigos maliciosos;
5.1.1.2. Garantir que novos códigos maliciosos são adequadamente investigados, tratados e protegidos pela ferramenta corporativa adotada pela empresa;
5.1.1.3. Garantir a divulgação sobre informações de ameaças, códigos maliciosos e medidas de proteção aos usuários.

6. Sanções e Punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma N-SI-006 foi aprovada pelo Comitê Gestor de Segurança da Informação em conjunto com a diretoria no dia 17/10/2022.

APÊNDICE H – NORMA DE ACESSO REMOTO

1. Introdução

1.1. A presente norma complementa a Política Geral de Segurança da Informação, definindo diretrizes para o acesso remoto a ativos, serviços e recursos computacionais da EMPRESA.

2. Propósito

2.1. Estabelecer diretrizes para o acesso remoto a ativos, serviços e recursos computacionais de propriedade da EMPRESA, garantindo níveis adequados de proteção aos mesmos.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. Concessão e uso do acesso remoto

4.1.1. O acesso remoto aos recursos de propriedade da empresa é restrito a usuários que necessitem do mesmo para execução de suas atividades profissionais;

4.1.2. A realização do acesso remoto fora do expediente normal de trabalho não implicará no pagamento de horas extras ao usuário, excetuando-se em casos onde for comprovada a solicitação do acesso por parte autorizada;

4.1.3. O usuário será o único responsável por toda ação executada com suas credenciais de acesso remoto, incluindo qualquer atividade não autorizada exercida por terceiros em posse de suas credenciais;

4.1.4. O acesso remoto será concedido com os privilégios mínimos necessários para execução das atividades laborais;

4.1.5. Equipamentos computacionais utilizados para acesso remoto devem possuir ferramentas para proteção contra códigos maliciosos aderentes às diretrizes da empresa, assim como firewall local ativo;

4.1.6. Em casos de acesso não autorizado, extravio, furto ou roubo de dispositivos computacionais que possuam o acesso remoto ao ambiente da EMPRESA habilitado, o usuário responsável deverá informar o ocorrido imediatamente ao Comitê Gestor de Segurança da Informação.

4.2. Concessão e uso do acesso remoto para terceiros

4.2.1. O acesso remoto poderá ser concedido a terceiros ou prestadores de serviço, caso seja necessário;

4.2.2. Para concessão e uso do acesso remoto para terceiros, devem ser observadas as seguintes regras:

4.2.2.1. O acesso remoto de terceiros à infraestrutura computacional da empresa somente poderá ser concedido após a efetivação do acordo de confidencialidade entre as partes;

4.2.2.2. A concessão do acesso deverá ser limitada automaticamente ao tempo necessário estimado à atividade, não excedendo um máximo de 30 (trinta) dias corridos por concessão;

4.2.2.3. O usuário terceiro, bem como a empresa onde o mesmo trabalha, serão os únicos responsáveis por toda ação executada com suas credenciais de acesso, incluindo qualquer atividade não autorizada exercida por outras partes de posse de suas credenciais;

4.2.2.4. O acesso remoto será concedido com os privilégios mínimos necessários para execução das atividades;

4.2.2.5. Equipamentos computacionais utilizados por terceiros para acesso remoto devem possuir ferramentas para proteção contra códigos maliciosos aderentes às diretrizes da empresa, assim como firewall local ativo;
4.2.2.6. Em casos de acesso não autorizado, extravio, furto ou roubo de dispositivos computacionais de terceiros que possuam o acesso remoto ao ambiente da EMPRESA habilitado, o usuário responsável deverá imediatamente informar o ocorrido ao Comitê Gestor.

4.3. Monitoramento do acesso remoto
4.3.1. Toda informação acessada, transmitida, recebida ou produzida através do acesso remoto à infraestrutura da empresa está sujeita a monitoramento, não havendo qualquer expectativa de privacidade por parte do usuário;
4.3.2. Durante o monitoramento de seus recursos, a EMPRESA se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, gravar, ler, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais, toda informação trafegada em sua rede.

5. Papéis e Responsabilidades
5.1. GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO
5.1.1. É responsabilidade da GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO:
5.1.1.1. Avaliar, aprovar ou negar solicitações para uso de acesso remoto aos recursos da EMPRESA;
5.1.1.2. Controlar e monitorar qualquer tipo de acesso remoto fornecido pela empresa;
5.1.1.3. Tratar eventuais tentativas de acesso não autorizados ou incidentes de segurança relacionados ao acesso remoto e, quando pertinente, reportar os mesmos ao Comitê Gestor de Segurança da Informação.

6. Sanções e Punições
6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões
7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma
8.1. A norma N-SI-007 foi aprovada pelo Comitê Gestor de Segurança da Informação em conjunto com a diretoria no dia 17/10/2022.

APÊNDICE I – NORMA DE RESPOSTA A INCIDENTES

1. Introdução

1.1. A presente norma complementa a Política Geral de Segurança da Informação, definindo as diretrizes para responder a eventos ou incidentes de segurança.

2. Propósito

2.1. Estabelecer diretrizes para garantir a resposta e tratamento adequados a incidentes de Segurança da Informação que estejam ou possam vir a impactar os ativos, serviços de informação ou recursos computacionais da EMPRESA.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. Incidentes de segurança da informação

4.1.1. Todas as ocorrências que possam vir a ter impacto negativo sobre os ativos, serviços de informação ou recursos computacionais da EMPRESA serão caracterizadas como um incidente de segurança da informação, devendo ser tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos itens afetados;

4.1.2. Os incidentes de segurança devem ser priorizados com base na criticidade dos ativos afetados, bem como na estimativa de impacto prevista;

4.1.3. Todos os incidentes ou suspeitas de incidente de segurança devem ser imediatamente comunicados ao Comitê Gestor de Segurança da Informação;

4.1.4. Na ocorrência de um incidente, os ativos com suspeita de terem sua segurança comprometida, devem ser isolados do ambiente corporativo, de forma a garantir a contenção do incidente;

4.1.5. A extensão dos danos do incidente de segurança deve ser avaliada para, em seguida, ser identificado o melhor curso de ação para erradicação completa do incidente e restauração dos ativos de informação afetados;

4.1.6. Após a erradicação completa do incidente, deve ser realizada uma revisão completa da ocorrência, identificando o nível real de impacto, vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de maiores ações para evitar a recorrência do incidente.

4.2. Disseminação de informação sobre incidentes de segurança da informação

4.2.1. Nenhum tipo de informação sobre incidentes e ocorrências de segurança poderá ser divulgado para entidades externas sem aprovação expressa e formal da diretoria.

5. Papéis e Responsabilidades

5.1. GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO

5.1.1. É responsabilidade da GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO:

5.1.1.1. Atuar como responsável por ocorrências e eventos de segurança e garantir a existência de recursos para identificar, escalar, mitigar, conter, e erradicá-los, bem como ações efetivas para recuperar o estado anterior dos ativos, serviços ou recursos computacionais afetados;

5.1.1.2. Aprovar qualquer tipo de comunicação ou disseminação total ou parcial de informações sobre ocorrências e incidentes de segurança da informação para qualquer parte ou público.

6. Sanções e Punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma N-SI-008 foi aprovada pelo Comitê Gestor de Segurança da Informação em conjunto com a diretoria no dia 17/10/2022.

APÊNDICE J – TERMO DE USO INTERNO

CONSIDERANDO que a EMPRESA disponibiliza a seus usuários ativos, serviços e recursos computacionais exclusivamente para o desempenho de suas atividades profissionais;

CONSIDERANDO que a EMPRESA é a única proprietária de todos ativos, serviços e recursos descritos e, dessa forma, sendo responsável por todos os custos com os mesmos, não existindo assim qualquer tipo de expectativa de privacidade no uso dos recursos mencionados;

CONSIDERANDO que a EMPRESA poderá ser seriamente impactada pela má utilização de seus ativos, serviços e recursos computacionais;

DECLARO QUE:

1. Tenho conhecimento e acesso a Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de Segurança da Informação necessários ao meu trabalho, que se encontram disponíveis no portal corporativo (https://www.sitedaempresa.com.br/pgsi.pdf), aos quais li na íntegra, tomando conhecimento e ciência de suas disposições;
2. Compreendi completamente os termos, diretrizes, conceitos e condições de uso Política Geral de Segurança da Informação, bem como as demais normas e procedimentos necessários ao meu trabalho, me comprometendo a cumprir integralmente as disposições constantes em tais documentos;
3. Estou ciente e de acordo que, tanto os ativos e serviços de informação quanto a infraestrutura tecnológica da EMPRESA poderão ser utilizados somente para fins exclusivamente profissionais e relacionados às atividades da organização;
4. Estou ciente que é realizado o monitoramento de todos os recursos de propriedade da empresa, assim como qualquer acesso ou comunicação ocorrida através de sua infraestrutura tecnológica;
5. Estou ciente que violações da Política Geral de Segurança da Informação, bem como suas demais normas e procedimentos são passíveis de sanções e punições, podendo incorrer em responsabilização legal nas esferas administrativas, cíveis e penal, nos termos da legislação em vigor;
6. Comprometo-me a não revelar, fato ou informações de qualquer natureza a que tenha conhecimento por forças das minhas atribuições, mesmo após o encerramento do contrato de trabalho com a EMPRESA.