CentralIT
Tecnologia em Negócios



COMPROMISSO COM A SEGURANÇA DA INFORMAÇÃO

Versão 2.0
Junho 2026

Sumário

1 OBJETIVO 4
1.1 Importância da informação 5
1.2 A política de Segurança da Informação, Segurança Cibernética e Proteção à Privacidade 6
1.3 Partes Interessadas 7
1.4 Uso de recursos corporativos 7
1.5 Palavra do Presidente do Conselho de Acionistas Central IT 8
2 GOVERNANÇA E GESTÃO DA SEGURANÇA DA INFORMAÇÃO 9
2.1 Responsabilidades sobre Segurança da Informação e Proteção de Dados Pessoais 9
2.1.1 Responsabilidades da Alta Direção 9
2.1.2 Gestor de Segurança da Informação 9
2.1.3 Usuário 10
2.1.4 Encarregado pelo Tratamento de Dados Pessoais 10
2.1.5 Comitê de Segurança da Informação e Proteção de Dados Pessoais 11
2.2 Tratamento de dados pessoais 12
2.3 Classificação da Informação 13
2.4 Transferências de informações 15
2.4.1 Canais de comunicação eletrônica 15
2.4.2 Relações com partes externas 15
2.5 Correio eletrônico 16
2.6 Gerenciamento de Acesso 16
2.6.1 Política de senha 17
2.6.2 Registro de usuários 17
2.6.3 Exclusão de usuários 17
2.6.4 Alterações do nível de acesso 17
2.6.5 Revisões do nível de acesso 17
2.6.6 Acessos de terceiros 18
2.6.7 Segregação de Funções 18
2.7 Segurança em Nuvem 18
2.8 Resposta a Incidentes de Segurança 19
2.9 Prontidão de TIC para continuidade de Negócio 19

2.10 Inteligência de Ameaças 19
2.11 Gerenciamento de Risco 20
2.12 Integração da Segurança da Informação em Projetos 20
3 SEGURANÇA DOS COLABORADORES 21
3.1 Divulgação da Política de Segurança da Informação, Segurança Cibernética e Proteção à Privacidade 21
3.2 Capacitação e Conscientização de Pessoal 21
3.3 Trabalho Remoto 21
3.4 Considerações - Direitos e Obrigações 22
4 SEGURANÇA FÍSICA 23
4.1 Política de mesa limpa e tela limpa 23
4.1.1 Política de mesa limpa 23
4.1.2 Política de tela limpa 23
4.2 Proteção de instalações e equipamentos compartilhados 23
4.3 Dispositivos Móveis 23
4.3.1 Regras básicas de utilização - Segurança de ativos fora das instalações da organização 24
4.4 Segurança Física 24
4.4.1 Áreas Seguras 25
4.5 Descarte e Destruição de Equipamentos e Mídias 26
4.5.1 Reutilização De Equipamento 26
5 SEGURANÇA TECNOLÓGICA 27
5.1 Backup das informações 27
5.2 Recursos de software 27
5.3 Criptografia 27
5.4 Sincronização de Relógios 28
5.5 Uso Seguro de Inteligência Artificial 28
6 GLOSSÁRIO 28

1 OBJETIVO

A Central IT estabelece uma política abrangente para a gestão da segurança da informação, delineando responsabilidades, padrões e procedimentos para mitigar os riscos relacionados à segurança da informação.

Atualmente a posse da informação significa enorme oportunidade de negócios, principalmente para uma empresa como a Central IT, que possui na informação o seu principal patrimônio.

Informação é um ativo que, como qualquer outro, tem muito valor para a organização e consequentemente necessita ser adequadamente protegido.

A informação pode ser disponibilizada de várias formas, podendo ser impressa ou manuscrita, armazenada eletronicamente, transmitida por correio ou por meios eletrônicos ou apresentar-se através de conversação. Seja qual for o meio pelo qual a informação é distribuída, partilhada ou armazenada, a mesma sempre requer proteções apropriadas.

A Segurança da Informação tem a função de proteger a informação de uma série de ameaças com o objetivo de zelar pela continuidade dos negócios, minimizar prejuízos e maximizar o retorno de investimentos e oportunidades de negócios. Desta forma, a segurança da informação torna-se responsável pela preservação dos seguintes aspectos da informação:

a) Confidencialidade: assegura que a informação permaneça acessível apenas a quem de direito;
b) Integridade: protege a exatidão e a totalidade da informação e das possíveis formas de processamento desta;
c) Disponibilidade: assegura que usuários autorizados tenham acesso à informação e aos ativos associados a ela quando necessário.

Fonte: ABNT NBR ISO/IEC 27002:2022

Para que a Segurança da Informação seja eficaz, depende do planejamento, análise e implementação de uma série de controles, compostos por políticas, práticas, procedimentos, estruturas organizacionais ou mecanismos eletrônicos e cada um tem responsabilidade internamente.

Neste documento, serão abordados os seguintes capítulos:

1. Capítulo 2 - Governança e Gestão da Segurança da Informação:
    a. Estabelece a base para a segurança da informação na organização.

   b. Inclui estrutura da gestão, política de segurança e gerenciamento de riscos.
2. Capítulo 3 - Segurança dos Colaboradores:
   a. Garante que os colaboradores estejam conscientes dos riscos e aptos a agir de forma segura.
   b. Abrange conscientização, treinamento, seleção e segurança de pessoal.
3. Capítulo 4 - Segurança Física:
   a. Protege os ativos físicos contra acessos não autorizados, danos e perda de dados.
   b. Inclui controle de acesso físico, segurança de equipamentos e continuidade de negócios.
4. Capítulo 5 - Segurança Tecnológica:
   a. Protege sistemas e dados contra-ataques cibernéticos, malware e outras ameaças tecnológicas.
   b. Abrange segurança de rede, recurso de software, controle de acesso, criptografia e sincronização de relógio.

1.1 Importância da informação

De forma crescente os sistemas de informações têm sido expostos a uma série de ameaças, dentre as quais podemos citar como exemplos, fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundações.

Desta forma podemos concluir que, nos parâmetros atuais, a segurança da informação é vital para a continuidade do negócio de qualquer organização, bem como dependente da participação ativa de todos os seus funcionários, seja em sua implementação e manutenção continua.

Todas as informações criadas, manuseadas, armazenadas, transportadas ou descartadas pelos colaboradores no exercício de atividades, sejam de propriedade da Central IT ou de terceiros, como fornecedores, clientes, parceiros e colaboradores, são de responsabilidade da Central IT. Essas informações devem ser protegidas adequadamente e não devem ser divulgadas, salvo quando permitido.

A Central IT reconhece a informação como um dos seus ativos mais valiosos, sendo o pilar fundamental para a inovação, a confiança dos clientes e a sustentabilidade do negócio. Como uma organização que atua na transformação digital e inteligência artificial, a integridade, a confidencialidade e a disponibilidade da informação não são apenas requisitos de segurança, mas diferenciais competitivos.

A proteção destes ativos é um compromisso da Alta Direção e uma responsabilidade compartilhada por todos os colaboradores, parceiros e fornecedores. Esta política estabelece as diretrizes para a implementação, manutenção e melhoria contínua de um Sistema de Gestão de Segurança da Informação (SGSI) resiliente, destinado a preservar a confidencialidade, integridade e disponibilidade das informações da nossa organização e dados de nossos clientes sobre nossa responsabilidade, protegendo-as contra ameaças cibernéticas, incidentes acidentais, acessos não autorizados e demais riscos de segurança, garantindo a continuidade das operações e a conformidade com os requisitos contratuais, regulatórios e legais.

1.2 A política de Segurança da Informação, Segurança Cibernética e Proteção à Privacidade

Este documento constitui um instrumento essencial que oferece diretrizes detalhadas para orientar a organização no planejamento, definição e implementação de mecanismos abrangentes, como normas, procedimentos, padrões, controles e outros dispositivos. Esses recursos foram concebidos para respaldar e aprimorar as atividades relacionadas à segurança da informação, segurança cibernética e proteção da privacidade. Eles são especialmente direcionados para as áreas identificadas como de maior risco para os processos de negócios da organização, garantindo uma abordagem proativa e eficaz para mitigar possíveis ameaças e vulnerabilidades.

A política de Segurança da Informação, Segurança Cibernética e Proteção à Privacidade da Central IT foi definida refletindo o compromisso da Alta Direção em prover os recursos necessários para a manutenção de um Sistema de Gestão Integrado (SGI), orientado aos seguintes princípios:

- **Alinhamento Estratégico e Prestação de Serviços:** A segurança da informação é o alicerce para a excelência na nossa prestação de serviços. Integramos proteção, resiliência e qualidade em toda a nossa estratégia de inovação em IA e transformação digital, garantindo que a confidencialidade, a integridade, a disponibilidade e a performance sejam inegociáveis em nossas entregas.
- **Melhoria Contínua:** A organização se compromete com a análise crítica periódica e a melhoria contínua, adaptando-o às mudanças no cenário de ameaças, à evolução tecnológica e ao crescimento do negócio.
- **Conformidade Normativa e Legal:** A Central IT assume o compromisso de satisfazer todos os requisitos legais, regulamentares (incluindo a LGPD) e

contratuais aplicáveis, tratando a conformidade como um requisito essencial de nossas operações e SLAs.

- **Cultura e Governança:** Esta política é o alicerce para todas as normas, procedimentos e manuais operacionais da organização. Ela deve ser comunicada, compreendida e aplicada por todos os colaboradores e partes interessadas, sendo sua violação passível de medidas disciplinares.

A avaliação da eficácia dos controles de segurança da informação será conduzida através de relatórios de auditoria interna visando assegurar que a proteção da informação e a qualidade do serviço evoluam em conjunto com os nossos objetivos de negócio. Esse processo ocorrerá, no mínimo, anualmente e sempre que necessário.

1.3 Partes Interessadas

A Central IT identifica como partes interessadas relevantes, entre outras, a Alta Direção, acionistas, colaboradores, clientes, fornecedores, parceiros, órgãos reguladores e demais partes com relação contratual ou legal com a organização.

As expectativas e necessidades dessas partes interessadas, especialmente as relacionadas à confidencialidade, integridade, disponibilidade, privacidade, continuidade dos serviços e conformidade legal e contratual, devem ser consideradas na definição, manutenção e melhoria do Sistema de Gestão de Segurança da Informação.

Sempre que aplicável, a Central IT deverá atender aos requisitos legais, regulatórios, contratuais e de negócio aplicáveis a cada parte interessada, conforme os processos, normas e procedimentos internos vigentes.

1.4 Uso de recursos corporativos

Os recursos de tecnologia da informação disponibilizados pela Central IT, incluindo e-mail, sistemas, internet, dispositivos, serviços em nuvem e quaisquer recursos fornecidos por terceiros em razão das atividades da organização, devem ser utilizados exclusivamente para fins profissionais e no interesse da Central IT.

É vedado o uso desses recursos para atividades que comprometam a segurança da informação, a privacidade, a imagem institucional, a continuidade dos serviços ou a conformidade legal e contratual da organização.

Consideram-se usos indevidos, entre outros, o acesso não autorizado, a disseminação de conteúdo malicioso, a violação de direitos autorais, o compartilhamento indevido de informações sigilosas ou restritas, o uso de softwares não autorizados, a prática de

fraudes, a utilização de redes ou meios inseguros para troca de informações sensíveis, a personificação, a falsa identidade, a obtenção de senhas e dados privativos, a perseguição, as ameaças, os downloads não autorizados, a distribuição de códigos maliciosos e vírus, o acesso e a disseminação de materiais pornográficos, ofensivos, difamatórios, discriminatórios, preconceituosos e atentatórios à moral e aos bons costumes, a instalação de softwares piratas, a veiculação de opiniões político-partidárias ou religiosas, conteúdos ilegais de incitação à violência, spam, a distribuição de correntes de mensagens eletrônicas, os vazamentos intencionais de dados e qualquer ação que possa comprometer a confidencialidade, a integridade ou a disponibilidade das informações e dos serviços da Central IT.

A Central IT poderá monitorar, restringir ou revogar o uso de recursos corporativos sempre que necessário para proteção do ambiente, investigação de incidentes, atendimento a requisitos legais ou preservação da continuidade dos serviços.

As informações de caráter de identificação pessoal ou qualquer outro dado sensível particular de colaborador, cliente ou parte interessada têm sua privacidade respeitada, conforme requerido pela legislação e regulamentação aplicáveis.

1.5 Palavra do Presidente do Conselho de Acionistas Central IT

A Central IT reconhece que a segurança da informação, a proteção de dados pessoais e a excelência na prestação de serviços são fundamentais para a sustentabilidade do negócio, para a confiança dos clientes e para a continuidade das operações.

A Alta Direção reafirma seu compromisso com a implementação, manutenção e melhoria contínua do Sistema de Gestão de Segurança da Informação, assegurando os recursos necessários para o cumprimento desta política, das obrigações legais, regulatórias e contratuais aplicáveis e dos objetivos estratégicos da organização.

Contamos com o apoio de todos os colaboradores, parceiros e demais partes interessadas para que as diretrizes aqui estabelecidas sejam conhecidas, compreendidas e praticadas no dia a dia, contribuindo para a proteção das informações, a integridade dos serviços e a reputação institucional da Central IT.

Carlos Freitas

Presidente do Conselho de Acionistas

2 GOVERNANÇA E GESTÃO DA SEGURANÇA DA INFORMAÇÃO

2.1 Responsabilidades sobre Segurança da Informação e Proteção de Dados Pessoais

2.1.1 Responsabilidades da Alta Direção

As responsabilidades da Alta Direção são definidas e revisadas regularmente pelo Conselho de Acionistas, incluindo o cumprimento das seguintes atribuições:

a) Definição e comunicação dos objetivos estratégicos relacionados à segurança da informação e conformidade com as normativas de proteção de dados, garantindo a disseminação dessa cultura por toda a organização;
b) Atribuir responsabilidades específicas para a gestão de segurança da informação;
c) Garantia da disponibilização dos recursos necessários para implementar e fortalecer os controles de segurança;
d) Acompanhamento e avaliação constante da implementação de soluções de segurança, assegurando a eficácia e relevância dessas medidas diante das necessidades em evolução.

2.1.2 Gestor de Segurança da Informação

Compete ao Gestor de Segurança da Informação coordenar, apoiar e monitorar as ações relacionadas à segurança da informação e à proteção de dados pessoais, promovendo conscientização, acompanhamento de riscos, apoio à implementação de controles e suporte às áreas da organização. A função de gestor de segurança da informação é revista sempre que necessário pela alta direção e visa a execução das seguintes tarefas:

a) Planejamento e condução de conscientização periódicos com o objetivo de disseminar a cultura de segurança dentro da Central IT, bem como de comunicar as atualizações eventualmente efetuadas na Política de Segurança da Informação, Segurança Cibernética e Proteção à Privacidade;
b) Apoio à equipe de infraestrutura na identificação dos ativos da Central IT e os responsáveis;
c) Monitoração do atendimento aos padrões, diretrizes e procedimentos vigentes em conjunto com a qualidade;
d) Acompanhamento das vulnerabilidades, dos pontos fracos existentes, dos riscos e ameaças eventualmente identificadas em auditorias de segurança, em conjunto com a qualidade;

e) Implementação de controles com o auxílio dos Gerentes e coordenadores de cada área, em conjunto com a qualidade;
f) Acompanhamento da implementação de soluções de segurança;
g) Apoio à qualidade na condução de revisões periódicas de segurança a fim de garantir que a política esteja sendo adequadamente seguida.

2.1.3 Usuário

Entende-se por usuário qualquer pessoa que utiliza os sistemas, aplicativos ou recursos de tecnologia da informação fornecidos pela Central IT para realizar suas tarefas ou atividades relacionadas ao trabalho. Isso inclui funcionários, contratados, clientes ou qualquer outra pessoa autorizada a acessar e utilizar os recursos de TI da Central IT, para cumprir suas funções.

As responsabilidades dos usuários são:

a) Proteger a integridade, disponibilidade e confidencialidade dos ativos associados;
b) Reportar os incidentes e as fragilidades de segurança da informação e de privacidade e proteção de dados pessoais;
c) Seguir diretrizes, normas e políticas definidas de segurança de informação e de privacidade e proteção de dados pessoais.

2.1.4 Encarregado pelo Tratamento de Dados Pessoais

Compete ao Encarregado pelo Tratamento de Dados Pessoais atuar como canal de comunicação entre a Central IT, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD), além de orientar a organização quanto às práticas de proteção de dados pessoais e apoiar o tratamento de incidentes relacionados à privacidade.

Dentre as responsabilidades do Encarregado, estão:

a) Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
b) Receber comunicações da Autoridade Nacional de Proteção de Dados e adotar providências;
c) Orientar os colaboradores e os contratados da organização a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

d) Atender às atribuições determinadas pelo controlador, pela ANPD e/ou estabelecidas em normas complementares;

e) Apoiar a gestão dos incidentes que envolvam dados pessoais, garantindo o tratamento adequado e comunicando os envolvidos, conforme legislação aplicável;

f) Identificar e avaliar as ameaças à privacidade e proteção de dados, bem como propor, e quando aprovado, apoiar a implantação de medidas corretivas para as tratativas dos riscos;

g) Apoiar o Comitê de Segurança da Informação e Proteção de Dados Pessoais em suas deliberações;

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

2.1.5 Comitê de Segurança da Informação e Proteção de Dados Pessoais

Compete ao Comitê apoiar a governança da segurança da informação e da proteção de dados pessoais, analisando diretrizes, revisando documentos normativos, apoiando decisões estratégicas e promovendo a cultura de segurança e privacidade na organização.

O Comitê é composto por um grupo multidisciplinar da organização e é focado nos aspectos relacionados à privacidade e proteção de dados, além de prestar apoio ao Encarregado em suas atribuições.

Dentre as responsabilidades do Comitê, estão:

a) Analisar, revisar e aprovar políticas, normas, procedimentos etc., relacionados à privacidade e proteção de dados pessoais;

b) Auxiliar na implementação das mudanças a fim de mitigar os riscos relacionados à privacidade e proteção de dados;

c) Auxiliar na implementação de medidas de segurança desde a fase de planejamento de projetos, sistemas, processos, procedimentos etc.;

d) Auxiliar na manutenção da conformidade com as legislações através de métricas, controles, auditorias periódicas entre outros;

e) Zelar para que tratamento de dados pessoais seja realizado em conformidade com esta política e a legislação vigente;

f) Promover a divulgação desta política e tomar as ações necessárias para disseminar a cultura de privacidade e proteção de dados pessoais na organização;

g) Auxiliar na conscientização dos colaboradores sobre as políticas, normas, procedimentos etc., referentes à privacidade e proteção de dados pessoais;

h) Realizar reuniões periódicas.

i) Atuar como instância de governança em segurança da informação nos projetos da organização, estabelecendo diretrizes, orientando as áreas e, quando aplicável, realizando avaliações por criticidade ou amostragem, sem tirar a responsabilidade operacional na execução dos controles dos gestores das áreas da Central IT.

2.2 Tratamento de dados pessoais

A Central IT garante que o tratamento de dados pessoais será realizado de forma lícita, transparente, adequada e necessária, observando a legislação vigente, as finalidades legítimas previamente informadas e os princípios de segurança da informação, privacidade e proteção de dados pessoais.

Os dados pessoais deverão ser coletados, utilizados, armazenados, compartilhados, retidos e descartados de maneira compatível com a finalidade declarada e com os requisitos legais, regulatórios, contratuais e internos aplicáveis.

A organização adotará medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados, destruição, perda, alteração, comunicação ou divulgação indevida.

Sempre que aplicável, os titulares dos dados deverão receber informações claras e acessíveis sobre o tratamento realizado, e alterações relevantes deverão ser comunicadas quando exigido pela legislação.

O uso de tecnologias emergentes, inclusive soluções de Inteligência Artificial, no tratamento de dados pessoais deverá observar os princípios de privacidade, segurança da informação, rastreabilidade, governança e mitigação de riscos.

Nas atividades de tratamento de dados pessoais, são diretrizes da Central IT:

a) Expressar, de maneira clara, objetiva e adequada ao contexto, como os dados pessoais serão tratados para o titular, antes da primeira coleta ou utilização;

b) Fornecer aos titulares dos dados pessoais informações claras e de fácil acesso, conforme legislação vigente;

c) Garantir que as atividades de tratamento de dados pessoais estejam em conformidade com a legislação vigente aplicável;
d) Realizar a coleta de dados pessoais de acordo com a legislação vigente e com os objetivos especificados;
e) Reter dados pessoais apenas pelo tempo necessário para o cumprimento dos propósitos declarados e/ou para o cumprimento de obrigações legais;
f) Prezar pela qualidade dos dados pessoais tratados;
g) Tratar os incidentes que envolvam vazamentos de dados pessoais, garantindo que sejam devidamente registrados, classificados, investigados, corrigidos e documentados;
h) Disponibilizar políticas, normas, procedimentos, orientações e/ou práticas relacionadas à privacidade e proteção de dados pessoais a todas as partes interessadas e autorizadas, tais como colaboradores, parceiros, terceiros e/ou clientes, quando aplicável;
i) Adotar medidas técnicas e administrativas com o intuito de proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
j) Promover comunicação, treinamentos, palestras e/ou workshops, objetivando o fortalecimento da cultura de privacidade e proteção de dados na organização.
k) Melhorar continuamente os processos e atividades relacionados à privacidade e proteção de dados pessoais;
l) Zelar pela não discriminação dos indivíduos no tratamento de dados pessoais;
m) Comunicar aos titulares quando ocorrerem alterações significativas no tratamento dos seus dados pessoais;
n) O uso de tecnologias emergentes, incluindo soluções de Inteligência Artificial, no tratamento de dados pessoais deverá observar os princípios de segurança da informação, privacidade e conformidade legal, garantindo controle, rastreabilidade, inclusive o digital, e mitigação de riscos associados ao seu uso.

2.3 Classificação da Informação

O processo de classificação e rotulagem das informações é fundamental para proteger os ativos de informação da Central IT, assegurando que o nível de proteção, acesso, compartilhamento, armazenamento e descarte seja compatível com a sensibilidade, criticidade e requisitos legais aplicáveis.

A seguir, apresentamos um resumo das classificações de informações na Central IT.

Nível	Descrição	Quem pode classificar	Quem acessa	Rótulo
Pública	Documentos e informações que o acesso é permitido a todas as pessoas.	Assessoria de Qualidade	Qualquer pessoa, interna ou externa, à Central IT	Público
Acesso Interno	Documentos e informações que contêm procedimentos e modelos utilizados pela Central IT.	Assessoria de Qualidade	Todos os colaboradores internos da Central IT	Interno
Restrita	Documentos que contenham informações de caráter pessoal, análises e tratativas com clientes, de relacionamento com fornecedores ou que sua divulgação interna possa causar prejuízos à Central IT no que se refere à sua reputação ou harmonia de funcionamento.	Assessoria de Qualidade	Apenas colaboradores internos da área, ou grupos de trabalho, onde é executado o processo, inclusive pessoas às quais o gestor da informação der acesso (inclusive clientes e fornecedores), assim como Diretores.	Restrito
Confidencial	Documentos que contenham informações estratégicas para a Central IT, incluindo prospecção de novos clientes ou que possam causar danos à imagem da Central IT ou prejuízos financeiros.	Assessoria de Qualidade	Apenas pessoas indicadas pelo gestor da informação.	Confidencial

Tabela 01 – Quadro para Classificação da Informação

As informações compartilhadas com fornecedores, clientes e outros agentes externos deverão ser tratadas conforme o nível de classificação definido, observando-se os controles necessários para evitar divulgação indevida. Quando a informação for produzida por agente externo, deverá ser respeitado o grau de restrição informado, ou aplicado nível mais restritivo, quando julgado necessário pela Central IT.

O tratamento dado pela Central IT às informações recebidas de agentes externos nunca poderá ser menos restritivo do que o indicado pelo emissor.

2.4 Transferências de informações

As informações da Central IT devem ser transferidas por meios seguros e compatíveis com sua classificação, observando as necessidades do negócio, os requisitos legais, regulatórios e contratuais aplicáveis, e os controles definidos pela organização.
A transferência de informações por canais eletrônicos, físicos ou verbais deve considerar a sensibilidade do conteúdo, o destinatário autorizado e o nível de proteção necessário para evitar acesso, alteração, perda ou divulgação indevida.
Sempre que houver compartilhamento de informações com partes externas, deverão ser adotadas medidas de proteção adequadas e, quando aplicável, formalizados instrumentos contratuais ou equivalentes que definam responsabilidades, autorizações, restrições, confidencialidade e resposta a incidentes.

2.4.1 Canais de comunicação eletrônica

As informações da organização devem ser trocadas por meio de canais de comunicação eletrônica corporativos aprovados pela Central IT, incluindo e-mail, Microsoft 365 corporativo, transferência de dados via FTP, telefones corporativos e sites corporativos internos ou externos, quando aplicável.

2.4.2 Relações com partes externas

Partes externas incluem os diversos fornecedores de serviços, empresas de manutenção de hardware e software, empresas que gerenciam transações, processamentos de dados ou clientes.
Caso haja necessidade de troca de dados confidenciais ou sigilosos com qualquer parte externa, o relacionamento deverá ser formalizado previamente por instrumento contratual ou equivalente, sob responsabilidade da área contratante.
O contrato poderá ser formalizado fisicamente ou em formato eletrônico e deve conter cláusulas que estejam de acordo com a avaliação de riscos, incluindo, no mínimo:

- O método de identificação do terceiro;
- As autorizações para acesso às informações;

- A garantia de não repúdio;
- As normas técnicas para transferência de dados;
- A resposta a incidentes;
- Os rótulos e a gestão de informações confidenciais ou restritas;
- Os direitos autorais;
- Sigilo e confidencialidade das informações acessadas durante e após o contrato.

Os contratos com as partes externas precisam ser definidos considerando:

- A anuência de requisitos de segurança da informação da Central IT por intermédio de, no mínimo, uma das opções: Assinatura do TERMO DE CIÊNCIA DA POLÍTICA DE SEGURANÇA DO FORNECEDOR, a inclusão de cláusulas de sigilo ou confidencialidade no contrato firmado ou Assinatura do termo de confidencialidade padrão Central IT;
- Seguir os princípios e regras básicas estabelecidas na POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA FORNECEDORES.
- O acesso fornecido será monitorado por intermédio dos controles de redes vigentes.

2.5 Correio eletrônico

O correio eletrônico corporativo deve ser utilizado exclusivamente como ferramenta de comunicação da Central IT, observando as diretrizes desta política e demais normas aplicáveis.

É vedado o uso do e-mail corporativo para assuntos pessoais ou para o tráfego inadequado de informações confidenciais, restritas ou de qualquer conteúdo que possa comprometer a segurança da informação, a privacidade, a imagem institucional ou a conformidade legal e contratual da organização.

Os usuários devem adotar cautela no envio, recebimento e encaminhamento de mensagens, assegurando que o conteúdo seja destinado apenas aos destinatários autorizados e que a classificação da informação seja respeitada.

2.6 Gerenciamento de Acesso

O acesso aos recursos, sistemas e informações da Central IT deve ser concedido com base no princípio do menor privilégio, observando a necessidade de negócio, a segregação de funções e os requisitos de segurança da informação e privacidade.

Todo acesso deve ser formalmente solicitado, aprovado, registrado, monitorado e revisto periodicamente, conforme os processos internos aplicáveis.

A concessão, alteração e revogação de acessos devem considerar a função, a responsabilidade do usuário, o vínculo com a organização e a classificação da informação.

2.6.1 Política de senha

As senhas de acesso aos sistemas e a contas de e-mail são pessoais, confidenciais, intransferíveis e de total responsabilidade do colaborador. Os colaboradores e terceiros são responsáveis por todas as ações feitas sob seu acesso e responderão civil e criminalmente por quaisquer abusos cometidos neste contexto.

2.6.2 Registro de usuários

O registro de novos usuários é realizado pelo processo interno competente, mediante solicitação formal e conforme as necessidades de acesso previamente aprovadas pela área responsável. A disponibilização dos acessos necessários à rede corporativa é de responsabilidade do suporte interno (Infraestrutura de TI) da Central IT.

Todo o processo é conduzido em conformidade com o Gerenciamento de Acessos, documento que estabelece as diretrizes para o registro, concessão, manutenção e revogação dos acessos corporativos, devendo ser rigorosamente observado.

2.6.3 Exclusão de usuários

Os acessos deverão ser revogados após o desligamento do colaborador ou encerramento do vínculo com a Central IT, bem como em caso de mudança que torne o acesso desnecessário ou incompatível com a função exercida.

2.6.4 Alterações do nível de acesso

As alterações nas atividades exercidas pelo usuário deverão ser formalizadas pelos canais corporativos definidos, para que os acessos sejam ajustados conforme a nova necessidade de trabalho.

2.6.5 Revisões do nível de acesso

Os acessos aos sistemas, visto sua importância para o negócio, periodicamente.

2.6.6 Acessos de terceiros

Os acessos concedidos a prestadores de serviço, terceirizados e demais terceiros deverão observar as condições contratuais, os termos de confidencialidade e os controles de segurança definidos pela Central IT.

Esses acessos deverão ser concedidos somente quando estritamente necessários e monitorados durante toda a sua vigência

2.6.7 Segregação de Funções

A Central IT adota o princípio da segregação de funções, assegurando que atividades críticas não sejam concentradas em uma única pessoa. As funções de autorização, execução, revisão e auditoria devem ser desempenhadas por indivíduos distintos, reduzindo o risco de erros, fraudes ou uso indevido de acessos. As responsabilidades devem ser atribuídas de forma clara, garantindo transparência, rastreabilidade e conformidade com os requisitos de segurança da informação, governança corporativa e proteção à privacidade.

2.7 Segurança em Nuvem

A Central IT estabelece diretrizes para o uso seguro dos serviços em nuvem, com o objetivo de prevenir incidentes que possam comprometer a segurança da informação, a continuidade dos serviços e as operações de negócio. Essas diretrizes estão de acordo com a POLÍTICA DE USO DE SERVIÇOS EM NUVEM, que define os padrões e práticas aceitáveis para o emprego seguro desses serviços.

O uso de serviços em nuvem deve observar a política específica da organização, bem como os requisitos legais, regulatórios, contratuais e técnicos aplicáveis, assegurando a integridade, confidencialidade e disponibilidade das informações.

Todos os colaboradores, terceiros e demais usuários autorizados devem compreender e seguir as diretrizes estabelecidas para o uso desses serviços, adotando práticas que reduzam riscos e preservem a postura de segurança da Central IT.

A política e os controles relacionados ao uso de serviços em nuvem deverão ser revisados periodicamente, visando manter sua aderência às necessidades do negócio e à evolução do cenário de ameaças.

2.8 Resposta a Incidentes de Segurança

A resposta a incidentes de segurança deve abranger a identificação, contenção, registro, análise, tratamento e encerramento do incidente, bem como a preservação das evidências necessárias e a comunicação às partes internas e externas competentes, quando aplicável.

Assim que o incidente for detectado, deve ser relatado o mais breve possível e formalizado por meio de procedimento específico INCIDENTES E REQUISIÇÃO DE SERVIÇOS.

Sempre que necessário, deverão ser adotadas ações de escalonamento, gestão de crises, análise pós-incidente e tratamento de vulnerabilidades relacionadas ao evento identificado.

2.9 Prontidão de TIC para continuidade de Negócio

Com o propósito de estabelecer diretrizes e objetivos para garantir a prontidão da Tecnologia da Informação e Comunicação (TIC) em situações de continuidade de negócio na Central IT, foi desenvolvido o Plano de Continuidade de Negócio (PCN), identificado como PLANO DE CONTINUIDADE DE NEGÓCIO - PCN. Este plano delineia os procedimentos e estratégias a serem seguidos em casos de interrupções não planejadas ou eventos que possam afetar a operação normal da empresa.

As medidas descritas neste plano têm como objetivo principal preservar a funcionalidade dos sistemas de TIC essenciais para as operações, assegurando a resiliência diante de possíveis interrupções, ao mesmo tempo em que se busca minimizar o tempo de inatividade e seus impactos nos serviços prestados pela organização.

A execução eficiente deste plano é crucial para garantir a rápida recuperação e retomada das atividades normais após eventos adversos.

2.10 Inteligência de Ameaças

A Central IT adotará processo contínuo de coleta, análise e interpretação de informações relacionadas a ameaças cibernéticas, com o objetivo de compreender, antecipar e mitigar riscos à segurança da informação.

Essa prática permitirá a identificação de padrões, comportamentos maliciosos e indicadores de comprometimento, apoiando ações proativas de prevenção, detecção e resposta a incidentes de segurança cibernética.

A inteligência de ameaça é essencial para fortalecer as estratégias de segurança, melhorar a postura defensiva e mitigar potenciais impactos adversos nos sistemas, conforme definidos na POLITICA DE INTELIGENCIA DE AMEAÇAS.

2.11 Gerenciamento de Risco

A Central IT conduzirá a gestão de riscos organizacionais em suas áreas internas e contratos, com o objetivo de mitigar impactos de eventos imprevisíveis e apoiar a tomada de decisão.

O processo de gerenciamento de riscos deverá identificar e mapear vulnerabilidades, analisar e classificar os riscos quanto à probabilidade e ao impacto, definir o tratamento adequado e estabelecer planos de ação correspondentes.

Durante essa análise, são também identificados os controles corporativos necessários, o tipo de tratamento adequado e os planos de ação correspondentes.

É realizado anualmente um contato com as áreas internas e contratos, visando revisar os riscos existentes, encerrar aqueles que não representam mais uma ameaça ativa e incluir novos riscos mapeados ao longo do ano.

As diretrizes desse processo estão delineadas no documento GESTÃO DE RISCOS.

2.12 Integração da Segurança da Informação em Projetos

A segurança da informação deve ser considerada nos projetos e iniciativas da Central IT desde sua fase de planejamento, sendo responsabilidade das áreas executoras assegurar a avaliação e implementação de controles adequados ao contexto.

A aplicação dos controles deverá seguir abordagem baseada em risco e proporcionalidade, considerando criticidade, complexidade e impacto ao negócio. A evidência da consideração dos requisitos de segurança deverá ser registrada por meio de documentação adequada, garantindo rastreabilidade e suporte a auditorias. As diretrizes desse processo estão delineadas no documento MANUAL DE GERENCIAMENTO DE SERVIÇOS CENTRAL IT.

3 SEGURANÇA DOS COLABORADORES

3.1 Divulgação da Política de Segurança da Informação, Segurança Cibernética e Proteção à Privacidade

A divulgação da Política de Segurança da Informação, Segurança Cibernética e Proteção à Privacidade, está de acordo com os processos já adotados pela Central IT para divulgação de outros documentos e políticas.

Todos os envolvidos na implementação da política, incluindo a alta direção, gerências, funcionários e terceiros, devem entender, conscientizar-se e comprometer-se com o conteúdo da política e de seus adendos, comprovando o atendimento a estes pré-requisitos formalmente, através da assinatura do "Termo de Confidencialidade e Sigilo" e ou do "Contrato Individual Trabalho a Título de Experiência". Desta forma, o termo em questão faz parte da documentação pessoal exigida pela área de Gestão de Pessoas para cada funcionário, bem como dos contratos exigidos pela Central IT aos terceiros e estagiários sempre que aplicável.

3.2 Capacitação e Conscientização de Pessoal

Com o objetivo de manter os colaboradores e prestadores de serviços (conforme julgue necessário) adequadamente cientes e preocupados com as ameaças à segurança das informações, a Central IT deve conscientizar seus colaboradores, sobre a utilização adequada de procedimentos de segurança, privacidade e proteção de dados.

As ações de conscientização e treinamento deverão ser planejadas e conduzidas pelas áreas responsáveis, em conjunto com as demais áreas competentes, conforme a necessidade da organização, mediante a treinamento obrigatórios aos colaboradores da organização.

3.3 Trabalho Remoto

O trabalho remoto deverá observar as diretrizes estabelecidas pela Central IT para a execução de atividades fora das dependências da organização. Porém, o trabalho remoto não pressupõe obrigatoriamente o uso de celulares/smartphones.

A implementação do trabalho remoto na Central IT disciplinou a forma de execução de atividades remotas através do termo de aditamento ao contrato de trabalho e termo de responsabilidade para teletrabalho. O mesmo é abordado POLITICA DE TELETRABALHO.

A Central IT estabelece diretrizes claras para a utilização de recursos computacionais particulares em sua rede corporativa, visando garantir a segurança e integridade dos dados. É expressamente proibida a inclusão ou utilização de equipamentos particulares ou de terceiros na rede corporativa sem o devido consentimento e autorização prévia da equipe de infraestrutura interna. Essa política se aplica a todos os colaboradores e prestadores de serviços que acessam a rede da Central IT.

Caso seja necessário o uso de um equipamento externo, é necessário seguir um procedimento específico. Primeiramente, devem solicitar autorização à equipe de infraestrutura interna, explicando a necessidade e o propósito do uso do equipamento. Em seguida, a equipe de infraestrutura fornecerá um meio seguro para o uso do equipamento externo, garantindo que não comprometa a segurança da rede corporativa.

É importante ressaltar que o não cumprimento desta orientação está sujeito a medidas disciplinares, dependendo da gravidade da violação. Além disso, violações graves podem acarretar procedimentos administrativos e, se aplicável, criminais.

3.4 Considerações - Direitos e Obrigações

O cumprimento da Política de Segurança da Informação e Proteção de Dados Pessoais e Comunicação é de responsabilidade de todos os Colaboradores e dos Prestadores de Serviços da Central IT, que devem proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada, bem como utilizar os recursos corporativos apenas para as finalidades aprovadas.

A violação das regras estabelecidas neste documento imputará punições e notificação às autoridades legais, em caso de cometimento de ações que violem leis civis, penais ou organizacionais.

Não será admitido manipular, alterar, deturpar e distribuir os dados, manuais, metodologias (as-built), códigos, documentos, marcas digitais, logotipos, banners, sinais, símbolos, ou os dispositivos de funcionalidade e proteção identificados como de direitos autorais, confidenciais, restritos, secretos, as que descrevem parte ou principal significante dos negócios da Central IT; as que contenham estratégias e direções de curto a longo prazo da Central IT, ou que venham concatenar valores, vantagens competitivas ou significantes, sobre qualquer tipo, aos concorrentes da Central IT.

A política, sempre que necessário, poderá ser modificada, desde que aprovada pela Diretoria da Central IT.

4 SEGURANÇA FÍSICA

4.1 Política de mesa limpa e tela limpa

As informações categorizadas como "Uso interno", "Restrito" e "Confidencial" foram classificadas de acordo com os critérios estabelecidos no documento CLASSIFICAÇÃO E ROTULAÇÃO DA INFORMAÇÃO.

4.1.1 Política de mesa limpa

Caso a pessoa autorizada não estiver no local de trabalho, todos os documentos em papel e todas as mídias de armazenamento de dados classificadas como confidenciais ou restritas devem ser removidas da mesa ou de outros locais (impressoras, copiadoras, etc.) para evitar o acesso não autorizado.
Mesmo em teletrabalho, deve-se ter os devidos cuidados com o vazamento indevido de informações. Esses documentos e mídias devem ser armazenados de forma segura.

4.1.2 Política de tela limpa

Se a pessoa autorizada não estiver em seu posto de trabalho, todas as informações confidenciais ou restritas devem ser removidas da tela e o acesso deve ser bloqueado a todos os sistemas aos quais essa pessoa possui autorização de acesso.
No caso de uma breve ausência (de até 10 minutos), é executada a política de tela limpa, implementada por meio de política de rede com bloqueio da tela, solicitando uma senha.

4.2 Proteção de instalações e equipamentos compartilhados

Documentos contendo informações confidenciais ou restritas deverão ser retirados imediatamente de impressoras, copiadoras e demais equipamentos compartilhados.
As instalações para envio e recepção de correspondências através das recepções são protegidas através de envelopes e classificadas através de protocolo.
O uso não autorizado de impressoras, copiadoras, escâneres e outros equipamentos compartilhados para cópias é controlado através do uso de PIN para liberar cópias e pela localização desses equipamentos em salas fechadas.

4.3 Dispositivos Móveis

Os dispositivos móveis compreendem todos os tipos de computadores portáteis e celulares/smartphones.

Não é permitida a inclusão ou utilização de equipamentos particulares ou de terceiros na rede corporativa da Central IT sem o devido consentimento e autorização prévia da equipe de infraestrutura interna. Caso seja necessário utilizar um equipamento externo, a equipe de infraestrutura deverá disponibilizar um meio seguro que não comprometa a segurança da rede da Central IT. O não cumprimento desta orientação está sujeito a procedimentos administrativos e criminais

De acordo com a regras básicas de utilização, tais equipamentos, somente deverão ser retirados das instalações da empresa após autorização.

4.3.1 Regras básicas de utilização - Segurança de ativos fora das instalações da organização

O colaborador que estiver portando dispositivos móveis, externamente às dependências da empresa, deverá se atentar para as seguintes regras:

a) As atualizações de patches de segurança e proteção contra códigos maliciosos são de responsabilidade da equipe de suporte de infraestrutura interna e deverão ser realizadas em intervalos regulares.
b) O colaborador que fizer uso de dispositivos móveis fora das instalações da empresa será necessário utilizar os meios de armazenamento corporativos (CITDocs ou outro local definido pela empresa).
c) Recomenda-se não armazenar informações confidenciais localmente em dispositivos móveis e/ou externos, como pendrives e HDs externos.
d) O colaborador não deve utilizar redes Wi-Fi públicas abertas para troca de informações sigilosas, confidenciais ou restritas.

Além disso, para garantir a segurança e a integridade das comunicações, recomenda-se o uso de uma conexão VPN (Virtual Private Network) ao acessar recursos da empresa fora de suas instalações físicas. A VPN proporciona uma camada adicional de proteção ao criptografar o tráfego de dados, tornando-o mais seguro contra possíveis interceptações por parte de terceiros.

4.4 Segurança Física

Procedimentos para controles, segurança e prevenção de acesso físico não autorizado são adotados pela Central IT, onde ambientes restritos possuem controle de acesso. Tais

procedimentos e controles são usados para proteger áreas como: centros de processamento de dados e salas com equipamentos de comunicação e fornecimento de energia.

4.4.1 Áreas Seguras

- **Controle de acesso predial:**

O controle de acesso físico é realizado através de:

1. Controles de entrada predial;
2. Recepção da Central IT identifica, acompanha e controla o acesso de visitantes e colaboradores nas áreas internas da Central IT, conforme descrito no RECEPÇÃO item 4.10;
3. Sistemas eletrônicos de controle de acesso que autorizam a entrada apenas de indivíduos portando o respectivo cartão de acesso;
4. Áreas seguras são protegidas por controles de acessos lógicos e/ou biométricos.

Para proteção do ambiente contra ameaças externas, além dos controles citados acima, também existem extintores de incêndio disponibilizados em locais apropriados, sprinklers por todo o andar que serão acionados caso haja indício de fumaça, câmeras de CFTV (Circuito fechado de televisão) para identificação dos transeuntes, além de estarem dispostas no ambiente placas de orientação para as saídas, áreas restritas e equipamentos de proteção.

A recepção centraliza a área de entrega e de carregamento de documentos e mercadorias, encaminhando o material aos devidos responsáveis, ou solicitando a presença do colaborador para acompanhamento do visitante.

- **Porta de saída de emergência**

Para fins de atendimento aos requisitos de segurança física e resguardar o bem-estar físico dos colaboradores e prestadores, a Central IT insere em suas rotinas de verificação de segurança física, das saídas de emergência e de alarmes.

- Vide MANUAL DE GERENCIAMENTO DE RECURSOS TECNOLOGICOS DA CENTRAL IT.
- Vide CHECK LIST MANUTENÇÃO PREVENTIVA DE SEGURANÇA.

- **Ameaças Externas e ambientais**

A fim de prevenir ou minimizar os impactos de eventos decorrentes de ameaças físicas e ambientais, como desastres naturais e outras ameaças físicas intencionais ou não intencionais à infraestrutura, a Central IT incorporou em sua análise de risco a avaliação dos seguintes aspectos, conforme descrito no documento GESTÃO DE RISCO:

- Proteção contra incêndios;
- Sobrecargas elétricas;
- Inundações;
- Terremotos;
- Explosões;
- Manifestações civis;
- Resíduos tóxicos;
- Emissões ambientais;
- Outras formas de desastres naturais ou causados por seres humanos.

Essa abordagem visa garantir a segurança e a continuidade das operações da Central IT diante de potenciais adversidades.

4.5 Descarte e Destruição de Equipamentos e Mídias

Dados e softwares licenciados armazenados em mídias móveis, como CD, DVD, pen drive, cartão de memória, computadores e notebooks, deverão ser permanentemente destruídos ou fisicamente inutilizados antes do descarte, de modo a evitar qualquer possibilidade de recuperação posterior.
O gerenciamento de mídias removíveis é realizado por meio do MANUAL DE GERENCIAMENTO DE MÍDIAS REMOVÍVEIS.

4.5.1 Reutilização De Equipamento

Para situações envolvendo a reutilização de equipamentos, estes serão submetidos a um processo de formatação prévia antes de serem reintegrados ao uso, conforme delineado nas diretrizes estabelecidas no documento MANUAL DE GERENCIAMENTO DE MÍDIAS REMOVÍVEIS.

5 SEGURANÇA TECNOLÓGICA

5.1 Backup das informações

A política de segurança da informação da Central IT visa proteger os dados da organização, garantindo sua disponibilidade e recuperabilidade em caso de falha de equipamento, destruição intencional de dados ou desastre. O objetivo principal do sistema de backup é gerenciar, em colaboração com os usuários, todas as informações críticas da Central IT que requerem cópias de segurança em fita e disco, definindo o momento de cópia, retenção, recuperação e descarte seguro da informação.

Todos os serviços e servidores em produção da Central IT são submetidos a backups, com especial atenção aos serviços críticos identificados, garantindo a restauração de acordo com as necessidades operacionais. Além disso, é fundamental que as cópias de segurança sejam testadas periodicamente para verificar sua integridade, conforme estipulado na política de backup PLANO OPERACIONAL DE BACKUP.

Para garantir a segurança dos dados, as cópias de segurança são armazenadas em locais externos, distantes e independentes das instalações físicas da organização, assegurando a proteção contra possíveis danos ou perdas.

5.2 Recursos de software

A instalação/atualização/remoção de softwares é de responsabilidade de equipe de suporte interno (infraestrutura de TI) da Central IT. Estes serviços quando necessários devem ser solicitados pelos canais de atendimento corporativo.

É expressamente proibida a remoção de sistemas de detecção, prevenção e eliminação de vírus de equipamentos móveis sem autorização da equipe de suporte interno (infraestrutura de TI) da Central IT.

Todo colaborador deve zelar pela segurança cibernética é física corporativa desta forma todo e qualquer aspectos que possa ser classificado como risco deve ser notificado pelos canais competentes e em casos que necessitem investigação, terem registro de incidente de segurança no ITSM Central IT.

5.3 Criptografia

A Central IT deverá adotar mecanismos de criptografia sempre que necessário para proteger informações, sistemas e comunicações, de acordo com sua classificação e criticidade. O uso de criptografia deverá seguir os padrões, diretrizes e controles definidos pela organização.

5.4 Sincronização de Relógios

Todos os computadores da rede da Central IT são sincronizados com um servidor de hora centralizado que ajusta o horário das estações sempre que ocorre a autenticação de entrada do usuário. É responsabilidade do suporte interno da Central IT, tomar as devidas providências para manter os sistemas de processamento da informação com a hora configurada de acordo com o servidor central de hora.

5.5 Uso Seguro de Inteligência Artificial

A utilização de soluções de Inteligência Artificial deve observar os princípios de segurança da informação, privacidade e governança, assegurando o uso responsável e compatível com as diretrizes da Central IT.

É vedada a inserção de dados internos não públicos, dados pessoais ou informações sensíveis em ferramentas de Inteligência Artificial não autorizadas.

Sempre que aplicável, o uso de soluções de Inteligência Artificial deverá considerar requisitos de rastreabilidade, controle, confidencialidade e mitigação de riscos.

6 GLOSSÁRIO

Autenticação: Processo de verificação da identidade de um usuário, sistema ou dispositivo antes da concessão de acesso a recursos ou informações.

Autorização: Processo de concessão de permissões de acesso a recursos, sistemas ou informações a um usuário ou dispositivo autenticado.

Classificação da informação: Processo de categorização das informações de acordo com seu nível de sensibilidade, criticidade e necessidade de proteção, considerando requisitos de confidencialidade, integridade e disponibilidade.

Confidencialidade: Propriedade da informação que assegura que ela esteja acessível apenas a pessoas, entidades ou processos autorizados.

Disponibilidade: Propriedade da informação ou do sistema que assegura seu acesso e uso quando necessário por pessoas autorizadas.

Dispositivo móvel: Equipamento portátil, como notebook, tablet ou smartphone, utilizado para acessar, armazenar, processar ou transmitir informações.

Encarregado pelo tratamento de dados pessoais: Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Incidente de segurança: Evento que comprometa ou possa comprometer a confidencialidade, integridade ou disponibilidade das informações, incluindo acessos não autorizados, vazamentos de dados e ataques cibernéticos.

Informação: Conjunto de dados organizados, processados ou não, que possuem valor para a organização e podem existir em meio físico, eletrônico, verbal ou visual.

Integridade: Propriedade da informação que assegura sua exatidão, completude e confiabilidade, protegendo-a contra alterações indevidas.

Mídias de armazenamento: Dispositivos físicos ou lógicos utilizados para armazenar dados, como discos rígidos, pen drives, cartões de memória, CDs, DVDs e outros meios equivalentes.

Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Política de senha: Conjunto de regras e requisitos definidos pela organização para criação, uso, alteração, proteção e gestão de senhas de acesso.

Recursos de tecnologia da informação: Ativos tecnológicos utilizados pela organização para coletar, processar, armazenar, transmitir, distribuir e utilizar informações, incluindo hardware, software, infraestrutura, serviços, processos e conhecimento associado.

Risco: Efeito da incerteza sobre os objetivos da organização, normalmente avaliado com base na probabilidade de ocorrência de um evento e em seu impacto potencial.

Segurança da informação: Conjunto de medidas técnicas, administrativas e organizacionais destinadas a proteger a confidencialidade, integridade e disponibilidade das informações.

Titular: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Tratamento de dados pessoais: Toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, armazenamento, compartilhamento, eliminação, avaliação ou controle da informação.

Teletrabalho: Modalidade de trabalho realizada fora das dependências físicas da organização, com uso de tecnologias de informação e comunicação.

Usuário: Pessoa que acessa ou utiliza, de forma legítima e autorizada, os ativos de informação, sistemas ou recursos tecnológicos da organização.