Título do Documento:

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Informações Importantes

FENOX TECNOLOGIA LTDA
Avenida Salmão, 325 - Salas 91 a 96 e 101
São José dos Campos - SP
CEP: 12246-260 - Brasil
(12) 3028-7644

www.fenoxtec.com.br
fenox@fenoxtec.com.br

INFORMAÇÕES DO DOCUMENTO

DADOS DO DOCUMENTO			
Título do Documento: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO **Título do Resumido:** P.S.I			
CONSIDERANDO a necessidade de garantir a proteção adequada das informações sob responsabilidade da organização, bem como assegurar que o tratamento, acesso, armazenamento, compartilhamento e descarte de tais informações ocorram de maneira controlada e conforme os princípios de confidencialidade, integridade e disponibilidade, esta *Política* tem por finalidade estabelecer diretrizes que orientem o comportamento, as responsabilidades e os controles aplicáveis à gestão da segurança da informação na Fenox Tecnologia			
Tipo: Documento Confidencial	**Numeração**: 23081045-P-SP		**Páginas**: 49
Área Emitente: Infraestrutura	**Distribuição**: ☒ Interno	☐ Externo	
Distribuído por: Qualidade	**Autor:** Jorge Luis Almeida	**Cliente:** FENOX	**Data:** 25/11/2025
Palavras Chaves: P.S.I	**Categoria:** Documento Confidencial		

REFERÊNCIA
Documentos de Referência: SG-MN-00 - Manual de sistema de Gestão Integrado e antigo SG-PL-04_04– Política de Segurança da Informação

DADOS DO PROJETO	
Cliente: FENOX TECNOLOGIA	**Projeto:** Unificação de codificação e armazenamento de documentação FENOX.

ELABORAÇÃO / REVISÃO

Rev.	Data	Ordem	Departamento	Quem	Justificativa	Status
00	17/04/23	Revisão	Infraestrutura / Qualidade	Filipe Soares André Luiz Santana	Revisão geral do texto, Item. 31 - Manutenção de Equipamentos 22 – Acessos Físicos: 22.1 - Entrada e Saída de Terceiros, Prestadores de Serviços, Fornecedores e Terceiros	Jorge Luis Almeida*
01	09/10/25	Revisão	Infraestrutura	Gabriel Souza	Revisão integral do texto, contemplando os itens 5 até 35 da SG-PL-04 –	P/ Aprovação

					Política de Segurança da Informação	
02	23/03/26	Revisão	Qualidade	LRM	Revisão de texto	P/ Aprovação

Índice

1 INTRODUÇÃO

Este documento tem por objeto estabelecer e divulgar as Políticas de Segurança da Informação. Para todos os colaboradores e prestadores de serviço, que estão envolvidos com as atividades da empresa e manipulam informação.

A Fenox Tecnologia tem o compromisso de garantir qualidade e confiabilidade em seus serviços prestados, levando confiança e excelência aos seus clientes e fornecedores.

Atualmente existem muitas informações expostas a muitas ameaças e vulnerabilidades, em virtude da grande conectividade e disponibilidade das informações na rede. Por isso, tornam-se imprescindível que as organizações se preocupem com o estabelecimento de controles, como as políticas, que protejam as informações da instituição e em casos mais graves que garantam a continuidade dos negócios.

Esta Política é formalmente aprovada pela Alta Direção da Fenox Tecnologia e possui caráter obrigatório, aplicando-se a todos os colaboradores, terceiros e partes interessadas que tenham acesso aos ativos de informação da organização.

O não cumprimento das diretrizes aqui estabelecidas será tratado como violação de segurança da informação, sujeito às medidas administrativas, contratuais e legais cabíveis

1.1 CONTEXTO DE SEGURANÇA DA INFORMAÇÃO

A Fenox Tecnologia atua em ambiente altamente regulado e dependente de tecnologia, processando informações críticas relacionadas a vistorias veiculares, incluindo dados pessoais, biometria, imagens e integrações com órgãos reguladores.

Nesse contexto, a segurança da informação deve considerar:

- ameaças cibernéticas e operacionais;
- riscos de indisponibilidade de serviços;
- requisitos regulatórios aplicáveis (DETRAN, CONTRAN, LGPD);
- dependência de infraestrutura tecnológica e serviços em nuvem.

A gestão da segurança da informação deve estar integrada aos processos de continuidade de negócios, gestão de riscos, proteção de dados pessoais e gestão de serviços, garantindo resiliência operacional e conformidade normativa.

2 OBJETIVOS

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da Fenox Tecnologia para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da empresa.

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC27002:2022, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

Com a intenção de aumentar a segurança da infraestrutura tecnológica direcionada ao uso corporativo, foi desenvolvida uma Norma de Segurança da Informação, visando a orientação de nossos colaboradores para a utilização dos ativos de tecnologia das informações disponibilizadas.

A Política de Segurança da informação define os princípios e as diretrizes que norteiam a segurança da informação na Fenox, estabelecendo quais controles de segurança serão aplicados e, ainda, as responsabilidades e competências na aplicação, gerenciamento e monitoramento dos controles definidos.

A Política de Segurança da Informação deve suportar o atingimento de objetivos mensuráveis, incluindo:

- proteção da confidencialidade, integridade e disponibilidade das informações;

- redução de incidentes de segurança da informação;
- conformidade com requisitos legais, regulatórios e contratuais;
- garantia de rastreabilidade e controle dos acessos e operações;
- suporte à continuidade dos serviços e operações críticas.

O desempenho desses objetivos deve ser monitorado por meio de indicadores definidos no âmbito do Sistema de Gestão Integrado.

A proteção de dados pessoais deve observar os princípios da LGPD, incluindo finalidade, adequação, necessidade, segurança, prevenção e responsabilização, sendo obrigatória a adoção de controles técnicos e administrativos que garantam a proteção dos direitos dos titulares e a rastreabilidade das operações realizadas.

3 PAPÉIS E RESPONSABILIDADES

A Segurança da Informação deve possuir papéis e responsabilidades formalmente definidos, documentados e atribuídos, sendo obrigatória sua implementação, monitoramento e revisão periódica.

Deve ser assegurado que:

- a Alta Direção aprove formalmente esta política, assegure recursos e avalie periodicamente sua eficácia;
- a área de Tecnologia da Informação implemente e opere os controles de segurança, mantendo evidências de sua execução;
- os gestores garantam a aplicação dos controles em suas áreas e validem acessos e responsabilidades;
- o responsável pelo SGI conduza auditorias, monitore conformidade e registre não conformidades;
- colaboradores e terceiros cumpram integralmente as diretrizes estabelecidas, mediante aceite formal.

As responsabilidades convêm estar vinculadas a registros formais (ex.: matriz de responsabilidades, descrições de função ou controles do SGI), sendo passíveis de verificação em auditoria.

A ausência de definição, atribuição ou evidência de responsabilidade deve ser tratada como não conformidade.

4 DEFINIÇÕES

Definição	Descrição
Ameaça	Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização. (ISO/IEC I27000, 2018).
Ativo	Qualquer coisa que tenha valor para a organização. (NBR ISO/IEC 27002, 2013)
Ativo de Informação	Dados, informações e conhecimentos obtidos, gerados, tratados e/ou armazenados na empresa. Exemplos desses ativos: base de dados, arquivos, contratos, acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos e planos institucionais, processos de trabalho entre outros.
Ativo de Tecnologia da Informação	Composto por ativos de software e ativos físicos, permitindo o armazenamento, a transmissão e processamento das informações. Entre os ativos de software podemos citar os aplicativos, sistemas, ferramentas de desenvolvimento e utilitários.

Definição	Descrição
Controle de Acesso	Conjunto de procedimentos, recursos e meios utilizados com a finalidade de garantir que os acessos aos ativos só ocorrerão após autorização e serão restritos, baseados nos requisitos de segurança e nas atividades do usuário. (ISO/IEC I27000, 2018)
Colaboradores	Funcionários CLT, estagiários, terceirizados contratados.
Confidencialidade	Nenhuma informação estará disponível ou será divulgada a entidades (pessoas, sistemas ou órgãos) não autorizadas.
Criticidade	Medida de risco obtida da combinação entre o possível impacto na Instituição ou em um projeto e a probabilidade de ocorrência de um evento que afete o mesmo.
Divulgação	Ato de tornar público as informações que circulam internamente.
Infraestrutura de TI	Instalações prediais, equipamentos, computadores, software, redes, telecomunicações, sistemas de armazenamento e recuperação de dados, aplicações computacionais, cabeamento, rede telefônica e de internet.
Mitigar/Reduzir o risco	Efetuar ações que reduzam a probabilidade, consequências negativas, ou ambas, associadas a um risco. (NBR ISO/IEC 27005, 2008).
Risco	Efeito da incerteza sobre os objetivos de segurança da informação e é associado com o potencial que as ameaças explorarão vulnerabilidades de um ativo de informação ou grupo de ativos de informação e, assim, causar danos a uma organização. (ISO/IEC I27000, 2018)
Segurança da Informação	Preservação da confidencialidade, da integridade e da disponibilidade das informações. (ISO/IEC I27000, 2018).
Sigilo	Confidencialidade, segredo.
Vulnerabilidade	Fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças. (ISO/IEC I27000, 2018)

Ação / Dispositivo	Abrange / Significa
Servidores	Dispositivos que fornecem serviços a aplicações, ferramentas de usuário e redes de computadores.
Sistema FENOX	Aplicativo de software, desenvolvida pela FENOX Tecnologia Ltda., utilizada para assegurar a disponibilidade, integridade e confidencialidade de dados e de informação quando da identificação de digital biométrica e facial de vistoriadores,

Ação / Dispositivo	Abrange / Significa
	preenchimento de formulários eletrônicos, carga de dados e imagens coletadas durante cada vistoria, consulta às bases de dados do DETRAN e emissão do Laudo de Vistoria Veicular. O Sistema assegura a uma comunicação exclusiva com o DETRAN, sendo vedada toda comunicação referente a qualquer dado ou informação vinculada ao laudo por parte da ECV.
Datacenter backup	Plataforma e infraestrutura computacional criada contratada com o propósito de viabilizar a implantação e manutenção de aplicações e serviços virtualizados mediante a utilização de uma rede mundial de centros de dados proprietários.
IPS	IPS (Sistema de Prevenção de Intrusos) são soluções físicas ou de software utilizadas para detectar tráfego malicioso para prevenir a presença de intrusos e de eventos adversos que podem comprometer o funcionamento de serviços e de aplicações.
Suporte Técnico	Time de pessoas qualificadas, que realizam o atendimento de chamados e contatos de clientes.
“Mesa e Tela Limpa”	Política aplicada a mesas de trabalho e telas encontradas nas dependências da FENOX – SG-PL-01 – Política Mesa Limpa e Tela Limpa.
Telecomunicações e Rede	Sistemas interconectados que utilizam recursos técnicos específicos para realizar a transmissão ou recepção de voz ou de dados.
Gerenciamento e Suporte a Servidores.	Conjunto de atividades necessárias para assegurar o correto funcionamento para assim aperfeiçoar o desempenho de sistemas operacionais e de recursos de “hardware”.
Active Directory Services.	Recurso centralizado utilizado para realizar a administração de usuários, grupos, membros dos grupos, senhas e computadores em um determinado Domínio.
Mensageria e Correio Eletrônico.	Serviços de correio eletrônico e mensageria em tempo real.
BackOffice	Gestão Web do Sistema FenoxTec.
Tempo Médio de Resolução	Tempo médio utilizado na solução de uma demanda de usuário.
Link de comunicação	Dispositivos de conexão entre computadores, com a finalidade de permitir a transferência de dados.
Download	Ação de transferir dados de um computador remoto para um computador local.
Backup	Cópia de segurança.

Ação / Dispositivo	Abrange / Significa
Backup Incremental	Cópia de segurança que grava apenas os arquivos que foram modificados desde a última cópia.
“Backup Full”	Cópia de segurança completa, independente dos arquivos terem sido alterados ou não.
“Restore”	Restauração de dados realizada a partir de uma cópia de segurança.
“Switch”	Dispositivo que possui a finalidade de conectar dispositivos de rede.
Roteador	Dispositivo de rede que envia pacotes de dados entre redes de computadores.
CFTV	Sistema de monitoramento de ambientes.
IP	Sequência numérica que representa o endereço de um determinado dispositivo em uma determinada rede.
DNS	O Domain Name System (DNS) é um sistema de gerenciamento de nomes hierárquico e distribuído para computadores, serviços ou qualquer recurso conectado à Internet ou em uma rede privada. O DNS está baseado em nomes hierárquicos e permite a inscrição do nome do “anfitrião” (host) e seu IP.
DHCP	Serviço de rede responsável pela distribuição automática / dinâmica de endereços IP e outros parâmetros de configuração de rede.
Storage	Recurso tecnológico utilizado para o armazenamento de dados e de imagens.
HD	Hard disk ou disco duro de um computador tipo notebook ou de mesa (“desktop”).
Firewall	Sistema de segurança de rede que controla os dados recebidos e enviados de uma determinada rede, baseado em regras pré-definidas.

Os ativos de informação devem ser formalmente identificados, classificados, registrados e vinculados aos respectivos Itens de Configuração, assegurando rastreabilidade, definição de responsabilidade e controle conforme os requisitos do SGI

5 SIGLAS

Sigla / Termo	Abrange / Significa	Contexto de aplicação
PSI	Política de Segurança da Informação	Documento e diretrizes corporativas de segurança
ABNT	Associação Brasileira de Normas Técnicas	Referência normativa (ABNT NBR)

Sigla / Termo	Abrange / Significa	Contexto de aplicação
NBR	Norma Brasileira	Referência de normas ISO adotadas no Brasil
ISO	International Organization for Standardization	Referência de normas de gestão e segurança
IEC	International Electrotechnical Commission	Parte do conjunto ISO/IEC
ISO/IEC 27002:2022	Código de prática para controles de segurança da informação	Base de recomendações da PSI
ISO/IEC 27001:2022	Sistema de Gestão de Segurança da Informação (SGSI)	Base de controles citados (ex.: acessos)
ISO/IEC 27001:2013	Versão anterior da norma de SGSI	Citada no SGIS
ISO/IEC 27000:2018	Vocabulário e visão geral de SGSI	Fonte de definições (ameaça, risco etc.)
ISO/IEC 27005:2008	Gestão de riscos de segurança da informação	Fonte para “mitigar/reduzir risco”
SGIS	Sistema de Gestão Integrado de Serviços	Integra ISO 9001, ISO/IEC 20000-1 e ISO/IEC 27001
ISO 9001:2015	Sistema de Gestão da Qualidade	Referência integrada no SGIS
ISO/IEC 20000-1:2020	Sistema de Gestão de Serviços (TI)	Referência integrada no SGIS
TI	Tecnologia da Informação	Infraestrutura, ativos e controles técnicos
LGPD	Lei Geral de Proteção de Dados (Lei nº 13.709/2018)	Privacidade, retenção, tratamento de dados
DETRAN	Departamento Estadual de Trânsito	Integração e obrigações regulatórias do Sistema FENOX
CONTRAN	Conselho Nacional de Trânsito	Referência regulatória (retenção/obrigações)
ECV	Empresa Credenciada de Vistoria	Contexto de laudos e restrição de comunicação

Sigla / Termo	Abrange / Significa	Contexto de aplicação
NDA	Non-Disclosure Agreement (Acordo de Confidencialidade)	Requisito para cessão de informação a terceiros
BO	Boletim de Ocorrência	Exigido em furto/roubo de dispositivos
RH	Recursos Humanos	Notificação administrativa em incidentes e desligamentos
MDM	Mobile Device Management	Exemplo de bloqueio remoto/gestão de dispositivos
AD	Active Directory	Gestão de identidades, grupos, autenticação, políticas
Active Directory Services	Serviços do Active Directory	Administração centralizada de usuários e computadores
SFILE	File Server (servidor de arquivos)	Repositório corporativo com permissões e backup
SharePoint	Plataforma M365 de colaboração e documentos	Armazenamento autorizado de informação
OneDrive	Armazenamento corporativo M365	Armazenamento autorizado de informação
M365	Microsoft 365	Suíte corporativa (Outlook, Teams, SharePoint, OneDrive)
MFA	Multi-Factor Authentication (Autenticação multifator)	Proteção adicional de acesso (ex.: e-mail, acessos remotos)
VPN	Virtual Private Network (Rede privada virtual)	Acesso remoto seguro e integrações governamentais
BackOffice	Portal de gestão web do Sistema FenoxTec	Chamados, relatórios, rastreabilidade de acessos
IPS	Intrusion Prevention System (Sistema de Prevenção de Intrusos)	Controle de tráfego malicioso e proteção de serviços
CFTV	Circuito Fechado de TV	Monitoramento físico das instalações
CPD	Centro de Processamento de Dados	Área restrita (acesso controlado e logs)

Sigla / Termo	Abrange / Significa	Contexto de aplicação
pfSense	Firewall/roteador (software)	Controle de internet, regras, failover, segmentação
VLAN	Virtual LAN (Rede local virtual)	Segmentação de rede mencionada em controles
HA	High Availability (Alta disponibilidade)	Firewalls em redundância (pfSense 01/02)
DNS	Domain Name System	Serviço de nomes e endereçamento em rede
DHCP	Dynamic Host Configuration Protocol	Distribuição dinâmica de IP e parâmetros de rede
IP	Internet Protocol (endereço lógico)	Identificação de dispositivos na rede
NTP	Network Time Protocol	Sincronização de tempo para logs consistentes
USB	Universal Serial Bus	Portas de mídia removível (bloqueio padrão)
CD	Compact Disc	Mídia removível (tratamento e descarte)
DVD	Digital Versatile Disc	Mídia removível (tratamento e descarte)
HD	Hard Disk (disco rígido)	Armazenamento e descarte seguro
SSD	Solid State Drive	Armazenamento e descarte seguro
P2P	Peer-to-Peer	Conteúdo/uso proibido na rede corporativa
GPO	Group Policy Object	Aplicação de políticas via AD (bloqueios/controles)
USBFree	Política/GPO citada para bloqueio de USB	Controle técnico de mídias removíveis
BitLocker	Criptografia de disco (Microsoft)	Proteção de dados críticos em notebooks
7-Zip	Ferramenta de compactação com senha	Proteção de arquivos em exceções de mídia

Sigla / Termo	Abrange / Significa	Contexto de aplicação
SLA	Service Level Agreement	Indicadores e relatórios de atendimento
SJC	São José dos Campos	Local do datacenter principal no texto
Azure	Microsoft Azure	Ambiente de contingência em nuvem
Cloudflare	Serviço de proteção e otimização de tráfego	WAF, DNS, CDN, DDoS, redirecionamento
GoCache	Serviço de cache/CDN (redundância)	Redundância em caso de falha do Cloudflare
CDN	Content Delivery Network	Otimização/distribuição de conteúdo (Cloudflare)
WAF	Web Application Firewall	Firewall de aplicação web (Cloudflare)
DDoS	Distributed Denial of Service	Proteção contra ataques (Cloudflare)
RAID	Redundant Array of Independent Disks	Resiliência e tolerância a falhas em storage
TB	Terabyte	Capacidade de discos nos storages
FSTG01 / FSTG02 / FSTG03	Identificadores internos de storages	Inventário e arquitetura de armazenamento
FVMDB01/02	Identificadores internos de bancos/servidores	Exemplo de servidores internos autorizados
Cloudberry	Solução de backup	Rotina de backup corporativo
CrashPlan	Solução de backup	Backup de VMs e incrementais diários
URBAM	Urbanizadora Municipal de São José dos Campos	Logística de descarte físico
PEV	Ponto de Entrega Voluntária	Alternativa para descarte físico
Help Desk	Central de suporte	Solicitação de exceção/desbloqueio de mídia

Sigla / Termo	Abrange / Significa	Contexto de aplicação
SURI	Canal/ferramenta de abertura de chamado integrada	Entrada de demanda e integração com BackOffice
ID Home	Sistema de controle de acesso (porta/andar)	Controle de acesso físico do 9º andar
Panther	Sistema de alarme	Armar/desarmar, credenciais restritas

6 DISPOSITIVOS MÓVEIS

A Fenox Tecnologia reconhece a importância da mobilidade e da agilidade na comunicação entre seus colaboradores. Para isso, autoriza o uso de equipamentos portáteis corporativos, bem como o uso controlado de dispositivos pessoais mediante prévia autorização da área de Infraestrutura.

6.1 Definição

Considera-se **dispositivo móvel** todo equipamento eletrônico que possibilite mobilidade, seja de propriedade da Fenox ou aprovado formalmente pela Diretoria em conjunto com o setor de Infraestrutura, incluindo, mas não se limitando a:

- Notebooks;
- Smartphones;
- Tablets;
- Armazenamento portátil (pendrives, HDs externos, SSDs portáteis, etc.).

6.2 Responsabilidade do usuário

- O colaborador assume integral responsabilidade pelo uso adequado do dispositivo, devendo proteger as informações corporativas nele armazenadas.
- É vedada a instalação de softwares e aplicativos não autorizados pela área de Infraestrutura.
- Todo dispositivo deve possuir **senha de bloqueio automático**, de acordo com os padrões de complexidade definidos pela Fenox.
- É proibida qualquer tentativa de alteração não autorizada do sistema operacional ou de configurações de segurança.

O colaborador deve zelar pela **proteção física** do equipamento, prevenindo furtos, perdas ou danos, e comunicar imediatamente qualquer incidente ao gestor direto e à Infraestrutura
Os dispositivos móveis devemestar sujeitos a controle e monitoramento pela área de Infraestrutura, assegurando rastreabilidade de uso, associação ao usuário responsável e conformidade com os requisitos de segurança da informação.

Dispositivos que realizem tratamento ou armazenamento de dados pessoais devem possuir controles adicionais de proteção, incluindo restrição de acesso, mecanismos de bloqueio, e, quando aplicável, possibilidade de bloqueio ou remoção remota de dados.

A utilização de dispositivos sem controle, sem identificação de responsável ou sem aplicação de medidas mínimas de segurança deve ser tratada como não conformidade

6.3 Uso pessoal e acessórios

- O uso de dispositivos pessoais conectados à rede corporativa requer autorização prévia da Infraestrutura, que avaliará risco, aplicabilidade e medidas de segurança necessárias.
- Dispositivos não autorizados não poderão ser conectados à rede da Fenox em hipótese alguma.

O uso de dispositivos deve observar integralmente as diretrizes de uso aceitável dos ativos da informação, sendo vedada qualquer utilização que comprometa a segurança, a integridade das informações ou a conformidade regulatória.

Desvios devem ser registrados, analisados e tratados no âmbito do SGI.

6.4 Procedimentos em caso de incidente

- Em caso de furto ou roubo, o colaborador deve comunicar imediatamente o gestor direto, a área de Infraestrutura e registrar boletim de ocorrência (BO) junto às autoridades.
- O setor de Infraestrutura procederá com bloqueio remoto, quando aplicável (ex.: MDM, Exchange Online, Active Directory).
- A área de Recursos Humanos deverá ser notificada para providências administrativas.

Todos os incidentes convêm ser registrados em sistema oficial, contendo data, descrição, impacto e ações realizadas, assegurando rastreabilidade e evidência para auditoria.

Incidentes que envolvam dados pessoais devem ser tratados conforme os requisitos da LGPD, incluindo avaliação de impacto e comunicação quando aplicável.

6.5 Boas práticas de segurança física

Ao transportar ou utilizar dispositivos móveis, os colaboradores devem observar:

1. Nunca deixar o equipamento exposto em locais públicos sem supervisão.
2. Transportar notebooks em bagagem de mão em viagens aéreas.
3. Evitar deixar o equipamento em veículos estacionados, mesmo que no porta-malas.
4. Manter distância de líquidos, objetos que possam causar quedas e áreas de risco.
5. Sempre que possível, guardar o equipamento em cofres de hotel ou armários de segurança quando em viagem.

6.6 Termo de responsabilidade

Todo colaborador que receber, utilizar ou tiver acesso a dispositivos móveis, portáteis ou equivalentes disponibilizados pela Fenox deverá assinar o Termo de Responsabilidade de Equipamentos Portáteis, como condição obrigatória para uso.

A assinatura do Termo formaliza que o colaborador:

- possui ciência integral das políticas, diretrizes e orientações aplicáveis ao uso dos dispositivos;
- compromete-se a utilizar os equipamentos exclusivamente para finalidades autorizadas e relacionadas às atividades profissionais;
- responsabiliza-se pela guarda, uso adequado, integridade física e lógica do equipamento e das informações nele armazenadas;
- compromete-se a adotar práticas de segurança, confidencialidade e proteção de dados, prevenindo acessos não autorizados, perdas, danos, vazamentos ou uso indevido;
- concorda em comunicar imediatamente qualquer incidente, perda, furto, roubo, falha de segurança ou suspeita de comprometimento do equipamento ou das informações.

O Termo de Responsabilidade constitui evidência formal de conscientização, responsabilização individual e alinhamento às práticas de governança, segurança da informação, proteção de dados pessoais, continuidade das operações e gestão dos ativos corporativos.

O termo de responsabilidade deve ser mantido como evidência formal no âmbito do Sistema de Gestão Integrado, sendo obrigatória sua rastreabilidade, atualização quando aplicável e disponibilidade para auditorias internas e externas.

6.7 Sanções

O descumprimento das disposições estabelecidas nesta política, bem como das obrigações assumidas no Termo de Responsabilidade, poderá resultar na aplicação de medidas proporcionais à gravidade, recorrência e impacto da infração, incluindo, mas não se limitando a:

- advertência formal;
- restrição ou bloqueio de acesso a sistemas, informações ou recursos tecnológicos;
- recolhimento do equipamento corporativo;
- aplicação de medidas disciplinares internas;
- adoção de medidas administrativas, contratuais ou legais cabíveis.

As sanções serão aplicadas com base em critérios de razoabilidade, proporcionalidade e responsabilização, considerando os impactos à segurança da informação, à privacidade de dados pessoais, à continuidade dos serviços, à integridade dos ativos corporativos e ao cumprimento das obrigações legais e contratuais da organização.

As definições estabelecidas nesta seção devem ser utilizadas como referência obrigatória para interpretação, aplicação e auditoria dos controles de segurança da informação, assegurando padronização conceitual, consistência na aplicação dos processos e alinhamento com os requisitos normativos do SGI.

As violações devem ser registradas formalmente como não conformidades ou incidentes de segurança, sendo analisadas quanto à causa, impacto e recorrência, com definição de ações corretivas e preventivas conforme o SGI.

7 USO ACEITÁVEL DE ATIVOS DA INFORMAÇÃO

Definimos como **ativos de informação** todos os recursos, físicos ou digitais, tangíveis ou intangíveis, que suportam os processos de negócio e sustentam a prestação de serviços da organização, incluindo quaisquer itens sob sua propriedade, controle ou custódia.

São considerados ativos de informação, entre outros:

- dados e bases de dados (estruturados e não estruturados);
- documentos e registros, em qualquer formato (físico ou eletrônico);
- sistemas, aplicações, softwares e códigos-fonte;
- infraestrutura tecnológica (hardware, servidores, estações de trabalho e periféricos);
- redes, serviços de comunicação e componentes de conectividade;
- serviços em nuvem, ambientes hospedados e recursos contratados de terceiros;
- dispositivos móveis e mídias removíveis;
- credenciais, chaves, certificados, tokens e demais mecanismos de autenticação e autorização;
- configurações, parametrizações, integrações e logs;
- conhecimento intelectual, metodologias, modelos, procedimentos e demais conteúdos produzidos, adquiridos ou mantidos sob responsabilidade da organização.

Todo ativo de informação deve ser tratado de forma compatível com sua criticidade e com os requisitos de confidencialidade, integridade, disponibilidade e, quando aplicável, privacidade e continuidade dos serviços.

7.1 Principios gerais

Os ativos da informação são de propriedade da Fenox ou encontram-se sob sua custódia contratual, devendo ser utilizados **exclusivamente para fins profissionais**, em alinhamento com os objetivos de negócio, obrigações legais, contratuais e diretrizes internas da organização.

É expressamente vedado o uso de ativos da Fenox para:

- fins pessoais não autorizados;

- atividades ilícitas ou antiéticas;
- práticas que possam comprometer a imagem, a reputação, a segurança ou a continuidade das operações da organização.

O uso dos ativos deve respeitar, em todos os casos, os **níveis de classificação da informação** (Confidencial, Interno e Externo), aplicando-se controles, restrições de acesso, compartilhamento e armazenamento compatíveis com cada categoria, de modo a preservar a confidencialidade, integridade, disponibilidade e, quando aplicável, a privacidade das informações.

As informações que contenham dados pessoais devem ser tratadas conforme os princípios da LGPD, assegurando finalidade, necessidade, segurança, rastreabilidade e controle do acesso, sendo obrigatória a conformidade com os registros de tratamento definidos no âmbito do SGPI.

7.2 Responsabilidade do usuário

Os colaboradores são responsáveis por garantir que informações sigilosas, restritas ou setoriais sejam armazenadas **exclusivamente em ambientes autorizados** pela área de Infraestrutura, tais como:

- FileServer corporativo (SFILE), com permissões de acesso controladas;
- SharePoint e OneDrive corporativos (Microsoft 365);
- servidores internos oficialmente autorizados.

É **terminantemente proibido** o armazenamento de informações sigilosas ou corporativas:

- em dispositivos pessoais;
- em mídias removíveis não autorizadas;
- em serviços de nuvem externos ou contas pessoais (ex.: Google Drive pessoal, Dropbox, similares).

O compartilhamento de informações deve ocorrer **somente com usuários autorizados**, mediante concessão de acesso temporário ou controlado, respeitando perfis de segurança, princípio do menor privilégio e rastreabilidade das ações.

7.3 Controles técnicos

Os acessos aos ativos da informação são:

- provisionados, mantidos e revisados periodicamente nos diretórios corporativos e sistemas de gestão;
- concedidos de acordo com função, necessidade operacional e perfil de risco.

Registros de acesso, uso e modificações em informações classificadas podem ser coletados, monitorados e analisados para fins de auditoria, investigação, conformidade e melhoria contínua.

Em caso de desligamento, mudança de função ou término de vínculo, todos os acessos lógicos devem ser revogados e os ativos físicos devolvidos **de forma imediata**, garantindo a proteção das informações e a continuidade operacional.

O uso dos ativos de informação deve ser monitorado, registrado e passível de auditoria, assegurando evidência suficiente para verificação de conformidade, investigação de incidentes e suporte à melhoria contínua do Sistema de Gestão Integrado.

Qualquer utilização em desacordo com as diretrizes estabelecidas deve ser tratada como não conformidade ou incidente de segurança da informação, com registro formal, análise de causa e definição de ações corretivas.

8 GESTÃO DE ATIVOS

Os ativos devem estar vinculados aos serviços de tecnologia da informação que suportam, permitindo análise de impacto, gestão de mudanças, continuidade dos serviços e rastreabilidade no contexto do gerenciamento de serviços.

A Fenox mantém processos formais e integrados de gestão de ativos, com o objetivo de assegurar **rastreabilidade, segurança, disponibilidade e controle** de todos os recursos que suportam os negócios e a prestação de serviços.

São considerados ativos, entre outros:
hardware, software, dados, licenças, redes, dispositivos móveis, serviços em nuvem e quaisquer recursos tecnológicos ou informacionais utilizados pela organização.

“Os ativos possuem classificação de informação associada, incluindo identificação de tratamento de dados pessoais, assegurando que seu uso, acesso, armazenamento e compartilhamento estejam alinhados aos requisitos de segurança da informação e privacidade.

8.1 Inventário de ativos

Todos os ativos são registrados no Podio, por meio de aplicativos específicos que suportam o controle de seu ciclo de vida.

O inventário é mantido atualizado sempre que ocorrer:

- aquisição;
- movimentação;
- cessão ou atribuição a colaboradores;
- baixa definitiva ou descarte.

Cada ativo possui um responsável formalmente identificado no sistema, assegurando **accountability** e governança.

O responsável pelo ativo deve assegurar a correta utilização, classificação, proteção e atualização das informações registradas, sendo obrigatória a validação periódica dos dados do inventário.

A ausência de responsável definido ou de validação periódica deve ser tratada como não conformidade

8.2 Ciclo de vida do ativo

O ciclo de vida dos ativos segue etapas definidas e rastreáveis:

8.2.1 AQUISIÇÃO

Realizada por meio do módulo FNX-Compras, com registro do fluxo de compra, categorização do ativo e vinculação ao setor demandante.

8.2.2 CADASTRO, ATRIBUIÇÃO E MONITORAMENTO

Executado no módulo FNX-Suporte → Ativos, contemplando características técnicas, número de série, data de aquisição, custo, status e colaborador ou setor responsável.

8.2.3 BAIXA E DESCARTE

Ativos obsoletos, danificados ou fora de uso são formalmente baixados, seguindo procedimentos de descarte seguro e controlado, conforme aplicável.

A devolução, transferência ou descarte de ativos deve ser formalmente registrada, assegurando rastreabilidade, identificação do responsável, data e condição do ativo, sendo obrigatória a manutenção dessas evidências no sistema corporativo

8.3 Responsabilidades

- **Administrativo**: manter o inventário atualizado, aplicar políticas de uso, retenção e descarte seguro dos ativos.
- **Gestores de Área**: solicitar aquisições, validar entregas, acompanhar o uso e assegurar a devolução dos ativos em caso de desligamento.
- **Colaboradores**: utilizar os ativos conforme esta política, zelar por sua integridade e assinar o Termo de Responsabilidade quando aplicável.

8.4 Ativo tangiveis

- Todo ativo físico é identificado por etiqueta patrimonial vinculada ao cadastro no Podio.
- Auditorias internas ou externas podem ser realizadas para validação do inventário físico em relação ao sistema.
- Evidências incluem, entre outras:
  relatórios do Podio (FNX-Suporte, FNX-Indicadores), termos de responsabilidade, registros de movimentação e protocolos de descarte.

8.5 Ativos intangíveis

Ativos intangíveis são registrados exclusivamente no Podio, não possuindo identificação física incorporada ao ativo.

São considerados ativos intangíveis, entre outros:

- licenças de software;
- contratos com ECV, fornecedores e colaboradores;
- documentos e registros do Sistema de Gestão Integrado;
- políticas, procedimentos, metodologias e demais informações institucionais relevantes.

Esses ativos devem receber o mesmo nível de controle, proteção, rastreabilidade e governança aplicável aos ativos físicos, conforme sua criticidade e uso.

Os ativos devem ser classificados quanto à criticidade, considerando impacto na continuidade dos serviços, segurança da informação, requisitos regulatórios e tratamento de dados pessoais.

Ativos críticos devem possuir controles reforçados, incluindo monitoramento, restrição de acesso, priorização em recuperação e integração com planos de continuidade.

Ativos que envolvam dados pessoais devem estar vinculados aos registros de tratamento definidos no RoPA, assegurando rastreabilidade, definição de base legal e controle das operações realizadas.

9 CLASSIFICAÇÃO, ROTULAGEM E CONTROLE DA INFORMAÇÃO

A classificação da informação na Fenox é um **mecanismo obrigatório de governança**, utilizado para definir **como a informação pode ser criada, armazenada, acessada, compartilhada, retida e descartada**, considerando riscos ao negócio, às pessoas, aos serviços e às obrigações legais.

Toda informação tratada pela organização deve possuir **classificação explícita ou implícita**, sendo vedado o tratamento de informação sem definição mínima de nível de sensibilidade.

A classificação é aplicada **independentemente do formato, meio ou tecnologia**, abrangendo documentos, sistemas, bancos de dados, mensagens, relatórios, registros operacionais, logs, integrações, backups e informações verbais.

9.1 Niveis de classificação

9.1.1 Confidencial

Informações críticas ou sensíveis cuja exposição, alteração ou indisponibilidade pode:

- comprometer a continuidade dos serviços;
- gerar impacto regulatório ou legal;
- causar danos financeiros, operacionais ou reputacionais;
- afetar direitos de titulares de dados.

Inclui, entre outros:
credenciais, chaves de acesso, dados pessoais sensíveis, registros regulatórios, planos estratégicos, relatórios de auditoria, informações de clientes e integrações externas. Acesso restrito, controlado, registrado e revisado.

9.1.2 Interno

Informações necessárias à operação da Fenox, destinadas ao uso interno, cujo compartilhamento externo não autorizado pode gerar impacto operacional ou organizacional.

Inclui:
procedimentos, instruções de trabalho, relatórios técnicos, documentos administrativos, registros de suporte e operação.

Acesso limitado a áreas, funções ou grupos definidos.

9.1.3 Externo / publico

Externo / Público
Informações aprovadas para divulgação externa, sem risco relevante ao negócio, desde que mantidas íntegras e atualizadas.

Inclui:
comunicados institucionais, materiais públicos, conteúdos do site, manuais destinados a clientes.

9.2 Rotulagem e identificação

A rotulagem tem função **preventiva e educativa**, permitindo que qualquer pessoa identifique rapidamente o nível de cuidado exigido.

- **Documentos físicos**: identificação obrigatória no cabeçalho ou rodapé.
- **Documentos digitais**:
  - controle primário por permissões de acesso;
  - identificação no nome do arquivo ou no conteúdo quando aplicável.
- **Sistemas e bases de dados**: classificação definida por ambiente, perfil de acesso e criticidade do dado.
- **E-mails**: uso obrigatório do disclaimer corporativo.
- **Informações verbais**: devem respeitar o nível de classificação do conteúdo tratado, incluindo local, público e contexto da comunicação.

9.3 Regras de tratamento por classificação

9.3.1 Informações confidenciais

- uso exclusivo em ambientes corporativos autorizados;
- vedado armazenamento em contas pessoais, dispositivos próprios ou serviços externos;

- compartilhamento apenas com necessidade comprovada;
- registro de acesso sujeito a monitoramento.

9.3.2 Informações internas

- armazenamento em ferramentas corporativas;
- compartilhamento restrito ao contexto profissional;
- vedada divulgação externa sem autorização.

9.3.3 Informações externas

- divulgação condicionada à aprovação da área responsável;
- manutenção de integridade e controle de versão.

9.4 Retenção, versionamento e eliminação

A retenção da informação deve estar **diretamente vinculada à finalidade**, obrigação legal ou necessidade operacional.

- documentos ativos: mantidos na versão vigente;
- versões anteriores: preservadas para rastreabilidade;
- eliminação: realizada somente por processo formal, com registro.

Nenhuma informação é eliminada de forma ad-hoc.

9.5 Responsabilidades

- **Infraestrutura**: controles técnicos, acessos, segregação, proteção e monitoramento.
- **Qualidade**: definição, padronização e conformidade documental.
- **Gestores**: validação do correto tratamento das informações da área.
- **Colaboradores**: uso adequado, respeito à classificação e reporte de desvios. É vedada a criação de cópias não autorizadas, exportação de dados críticos ou utilização fora dos ambientes corporativos definidos.

10 ARMAZENAMENTO E PROTEÇÃO DE DADOS CRÍTICOS

O armazenamento de dados críticos deve ser realizado de forma **controlada, segura e rastreável**, utilizando exclusivamente os **ambientes corporativos autorizados** e respeitando as diretrizes internas já definidas (classificação da informação, controle de acesso, rotinas de backup e gestão de mudanças).

Para este documento, considera-se “proteção” a aplicação conjunta de **controle de acesso**, **segregação**, **backup**, **registro de evidências**, **capacidade de recuperação** e **prevenção de cópias não autorizadas**, garantindo que os dados permaneçam disponíveis para operação, auditoria e obrigações regulatórias, sem exposição indevida.

Os dados críticos devem ser protegidos contra acesso não autorizado, vazamento, perda ou alteração indevida, sendo obrigatória a adoção de controles que assegurem confidencialidade, integridade, disponibilidade e rastreabilidade das informações.

Os dados críticos devem possuir classificação formal, incluindo identificação de dados pessoais quando aplicável, assegurando que seu armazenamento, acesso e tratamento estejam alinhados aos requisitos de segurança da informação e privacidade.

10.1 O que torna um dado crítico

Os dados classificados como críticos devem possuir classificação formal associada, incluindo identificação de dados pessoais quando aplicável, assegurando que seu tratamento esteja alinhado aos requisitos de segurança da informação e privacidade

Um dado é considerado crítico quando sua perda, alteração ou exposição pode:

10.1.1 Impactar a continuidade do negócio e a prestação de serviços

A indisponibilidade ou inconsistência desses dados pode comprometer a execução de processos essenciais, afetar a capacidade de atendimento aos clientes e prejudicar a operação regular dos serviços prestados. A dependência desses dados para suporte às atividades operacionais torna sua preservação necessária para garantir estabilidade, previsibilidade e retomada adequada das operações em caso de incidentes. Os dados críticos que contenham dados pessoais devem ser utilizados exclusivamente para as finalidades definidas, sendo vedado qualquer uso incompatível, não autorizado ou não registrado, conforme requisitos da LGPD.

10.1.2 Afetar obrigações regulatórias junto a órgãos como detran e contran

Esses dados sustentam o atendimento a requisitos legais, regulatórios e contratuais aplicáveis à atuação da organização. Sua perda, alteração ou acesso indevido pode resultar em inconsistências cadastrais, falhas em registros oficiais ou impossibilidade de comprovação de conformidade perante órgãos reguladores, impactando a relação institucional e o cumprimento de prazos e exigências formais.

10.1.3 Comprometer informações pessoais e sensíveis de clientes, colaboradores e parceiros

O tratamento inadequado desses dados pode gerar riscos à privacidade e aos direitos dos titulares, além de afetar a confiança depositada na organização. A proteção dessas informações é relevante para evitar exposição indevida, uso não autorizado ou interpretações incorretas que possam resultar em danos às pessoas envolvidas e à imagem institucional.

10.1.4 Gerar não conformidades em auditorias internas ou externas

A ausência, inconsistência ou falta de rastreabilidade desses dados pode dificultar a comprovação de controles, processos e decisões adotadas pela organização. Isso pode resultar em apontamentos de auditoria, recomendações corretivas ou necessidade de reprocessamento de informações, impactando a maturidade do sistema de gestão e os ciclos de melhoria contínua.

10.2 Ambientes autorizados

Dados críticos devem ser mantidos **preferencialmente** em ambientes corporativos controlados, com mecanismos de backup e rastreabilidade compatíveis com sua criticidade. A adoção desses ambientes visa preservar a disponibilidade, integridade e confidencialidade das informações, além de facilitar auditorias, investigações e processos de recuperação.

Incluem-se como ambientes corporativos controlados:

- **Repositórios de rede corporativos:** estruturas de pastas e diretórios institucionais com permissões gerenciadas e controle de acesso.
- **Servidores e bancos de dados internos:** bases e aplicações hospedadas em infraestrutura corporativa, com administração, segregação e monitoramento centralizados.
- **Plataformas corporativas de colaboração:** ambientes institucionais destinados a compartilhamento e trabalho colaborativo, com gestão de identidades, versionamento e permissões.

- **Soluções formais de backup e recuperação:** mecanismos corporativos que garantem redundância, capacidade de restauração e evidências mínimas do ciclo de proteção e recuperação dos dados.

10.3 Uso local e mobilidade

- armazenamento local é **operacional e temporário**;
- não substitui repositórios corporativos;
- não elimina obrigação de backup;
- não autoriza cópia pessoal.

Dados críticos **não pertencem ao dispositivo**, pertencem à organização.

A transferência ou cópia de dados críticos deve ocorrer exclusivamente por meios autorizados e controlados, sendo vedada qualquer movimentação que não possua rastreabilidade ou controle institucional.

10.4 Proteções aplicadas

- controle de acesso individual;
- segregação por função;
- criptografia quando aplicável;
- backups regulares, testados e rastreáveis;
- limitação clara do escopo de backup.

A integridade dos dados deve ser assegurada por mecanismos de verificação, garantindo que alterações não autorizadas sejam identificadas, registradas e tratadas.

O acesso aos dados críticos deve ser restrito com base no princípio da necessidade de negócio e menor privilégio, sendo obrigatória a vinculação do acesso à função do usuário e sua revisão periódica.

10.5 Responsabilidades

- **Infraestrutura**: segurança, backup, restauração, monitoramento.
- **Gestores**: garantir armazenamento correto dos dados da área.
- **Colaboradores**: não criar cópias paralelas, não exportar dados, não improvisar soluções.

Os dados pessoais classificados como críticos devem observar critérios de retenção, minimização e descarte seguro, conforme requisitos legais, regulatórios e diretrizes do Sistema de Gestão de Privacidade da Informação.

O armazenamento e a proteção dos dados críticos devem ser monitorados e passíveis de auditoria, sendo obrigatória a manutenção de evidências que comprovem a aplicação dos controles estabelecidos.
Os controles relacionados ao armazenamento e proteção de dados críticos devem possuir evidências associadas, incluindo registros de backup, acessos, restaurações e verificações, sendo passíveis de auditoria no âmbito do SGI.

11 CESSÃO DE ATIVOS DE INFORMAÇÃO DA FENOX

A cessão, o compartilhamento ou o acesso a ativos de informação da Fenox por terceiros é permitido exclusivamente quando necessário à execução de atividades de negócio, devendo ocorrer de forma controlada, rastreável e compatível com os requisitos de segurança da informação, privacidade e proteção de dados pessoais. A cessão ou compartilhamento deve ser formalmente registrado, assegurando rastreabilidade, identificação das partes envolvidas, finalidade, período de acesso e evidências associadas.

O compartilhamento de ativos de informação deve ser formalmente registrado, assegurando rastreabilidade das operações, identificação das partes envolvidas, finalidade, período de acesso e evidências associadas.

A Fenox adota o princípio da necessidade e minimização, assegurando que apenas as informações estritamente necessárias sejam compartilhadas, pelo menor tempo possível e com salvaguardas adequadas.

11.1 Definição

Consideram-se ativos de informação passíveis de cessão ou compartilhamento controlado:

- Documentos físicos ou digitais, incluindo procedimentos, relatórios técnicos, registros operacionais e evidências do SGI;
- Sistemas, aplicações, códigos-fonte, softwares próprios ou licenciados, quando previsto contratualmente;
- Bases de dados, relatórios ou extratos que contenham informações de clientes, colaboradores, fornecedores, parceiros ou órgãos reguladores;
- Qualquer outro ativo informacional sob custódia da Fenox que, por exigência contratual, regulatória ou operacional, precise ser acessado por terceiros.

11.2 Requisitos de confidencialidade e proteção de dados

- Informações classificadas como **Confidenciais** somente podem ser cedidas mediante **instrumento contratual formal**, incluindo cláusula de confidencialidade ou Acordo de Confidencialidade (NDA).
- O instrumento deve estabelecer, no mínimo:
- finalidade do compartilhamento; O compartilhamento de dados pessoais deve estar associado a base legal definida, devidamente registrada e compatível com a finalidade informada, conforme requisitos da LGPD.
- escopo e tipo de informação;
- responsabilidades das partes;
- medidas mínimas de proteção;
- prazo de retenção e critérios de descarte;
- consequências em caso de uso indevido.
- Quando envolver **dados pessoais**, o compartilhamento deve observar a **LGPD**, garantindo:
- base legal aplicável;
- definição clara de papéis (controlador, operador ou compartilhamento);
- uso compatível com a finalidade informada;
- adoção de medidas técnicas e administrativas adequadas pela parte receptora.

Os terceiros convêm atender aos requisitos de segurança da informação estabelecidos pela organização, sendo obrigatória a avaliação, monitoramento e responsabilização quanto ao tratamento adequado das informações compartilhadas.

Os terceiros envolvidos convêm atender aos requisitos de segurança da informação estabelecidos pela organização, sendo obrigatória a avaliação, monitoramento e responsabilização quanto ao tratamento adequado das informações compartilhadas.

A transferência de informações deve ocorrer exclusivamente por meios autorizados e controlados, sendo vedada qualquer forma de compartilhamento sem rastreabilidade ou proteção adequada contra vazamento ou acesso não autorizado.

A transferência de informações deve ocorrer exclusivamente por meios autorizados e controlados, assegurando proteção contra vazamento, interceptação ou acesso não autorizado, com rastreabilidade das operações realizadas.

11.3 Softwares, sistemas e licenças

- A cessão, acesso ou uso de softwares e sistemas somente ocorre quando houver **direito legítimo de uso**, respeitando contratos de licenciamento e restrições do fornecedor.

- É vedada a reprodução, cópia, redistribuição ou acesso não autorizado a softwares, códigos ou sistemas sob custódia da Fenox.
- O acesso concedido a terceiros deve ser **individual, rastreável e revogável**, sempre que possível por meio de perfis e controles técnicos.

11.4 Monitoramento avaliação jurídica, técnica e operacional

- Toda cessão de ativos de informação deve ser previamente avaliada quanto a:
- riscos legais e contratuais;
- impactos à segurança da informação e à privacidade;
- aderência às políticas internas e ao SGI.
- A Infraestrutura avalia os **meios técnicos de compartilhamento**, incluindo uso de canais seguros, controle de acesso, autenticação e registro de evidências.

11.5 Responsabilidades

- **Área Solicitante**: justificar a necessidade do compartilhamento e respeitar as restrições definidas.
- **Jurídico/Compliance (quando aplicável)**: validar instrumentos contratuais e cláusulas de confidencialidade.
- **Infraestrutura / Segurança da Informação**: definir meios seguros, registrar evidências e garantir rastreabilidade.
- **Terceiros**: cumprir integralmente as obrigações contratuais e legais assumidas.

Ao término da relação com terceiros, deve ser assegurada a devolução ou eliminação dos dados compartilhados, conforme aplicável, com registro formal da operação e manutenção de evidências.

As operações de cessão e compartilhamento devem ser monitoradas e passíveis de auditoria, sendo obrigatória a manutenção de evidências que comprovem a conformidade com os requisitos estabelecidos.

As operações de cessão e compartilhamento devem ser monitoradas e passíveis de auditoria, sendo obrigatória a manutenção de evidências que comprovem a conformidade com os requisitos estabelecidos.

12 TRATAMENTO DE MÍDIAS REMOVÍVEIS

A Fenox adota como diretriz o **não uso de mídias removíveis**, considerando os riscos de vazamento de informações, perda de rastreabilidade e introdução de códigos maliciosos no ambiente corporativo.

O uso de mídias removíveis deve ser previamente autorizado e justificado, sendo vedada sua utilização sem autorização.

12.1 Definição

São consideradas mídias removíveis:

- Pendrives, HDs e SSDs externos;
- Cartões de memória;
- CDs, DVDs e mídias ópticas;
- Fitas ou dispositivos portáteis de backup;
- Qualquer dispositivo de armazenamento portátil fora do controle padrão da Infraestrutura.

12.2 Política de uso

- O uso de mídias removíveis é **proibido por padrão**.
- Exceções somente são permitidas mediante **autorização formal da Infraestrutura**, devidamente justificada.
- A transmissão de informações deve priorizar **ferramentas corporativas autorizadas**, como SFILE, SharePoint, OneDrive corporativo, Teams, e-mail institucional e VPN.
- É vedado o uso de mídias pessoais em equipamentos corporativos.

12.3 Riscos e tratamento de incidentes

- Qualquer incidente envolvendo mídia removível é tratado como **incidente de segurança da informação**, podendo envolver:
- perda ou vazamento de dados;
- exposição indevida de dados pessoais;
- comprometimento de sistemas.
- Os incidentes seguem o fluxo formal de registro, análise e tratamento no SGI.

12.4 Descarte e reutilização

- Mídias com informações sensíveis devem ser descartadas de forma **irreversível e segura**.
- O descarte ou destruição deve ser **registrado no Pódio**, garantindo rastreabilidade.
- Dispositivos defeituosos com dados sensíveis não devem ser enviados para reparo sem avaliação prévia da Infraestrutura.

O descarte de mídias removíveis deve ser realizado de forma segura, assegurando a eliminação definitiva das informações, com registro formal da operação e manutenção de evidências.

12.5 Controles técnicos

- Controles técnicos, como **GPOs de bloqueio de USB**, são aplicados como padrão.
- Exceções são temporárias, registradas e monitoradas.

12.6 Conformidade legal

Todos os envolvidos devem observar a LGPD, contratos vigentes e regulamentações aplicáveis aos serviços da Fenox.

12.7 Descarte de informações e mídias

O descarte de informações e mídias deve garantir que os dados **não possam ser recuperados, reutilizados ou acessados indevidamente**.

12.8 Autorização e registro

- O descarte deve ser autorizado e **registrado formalmente**, com identificação do item, responsável e método aplicado.

12.9 Documentos em papel

- Documentos devem ser destruídos por fragmentação adequada.
- É proibido o descarte de documentos sensíveis em lixo comum.

12.10 Dispositivos de armazenamento

- Dispositivos devem ser inutilizados por destruição física ou sobrescrita segura.
- Quando houver risco elevado, a destruição física é mandatória.

12.11 Mídias relacionadas a órgãos reguladores

- Mídias ligadas a processos regulatórios devem ser avaliadas antes do descarte, podendo ser mantidas como evidência.

12.12 Logística de descarte

- O descarte físico é realizado por meios oficiais (URBAM ou PEV).
- Sempre que possível, deve haver **protocolo ou evidência do descarte**.

12.13 Responsabilidades

- **Infraestrutura**: avaliar e autorizar descarte.

- **Gestores**: validar retenção ou descarte.
- **Colaboradores**: encaminhar materiais pelos canais oficiais.

Quando envolver dados pessoais, o uso de mídias removíveis deve observar controles adicionais de proteção, assegurando confidencialidade, rastreabilidade e conformidade com a LGPD.

O uso, transporte e descarte de mídias removíveis devem ser monitorados e passíveis de auditoria, sendo obrigatória a manutenção de evidências que comprovem a aplicação dos controles.

13 DISPOSITIVOS DE MÍDIA REMOVÍVEL

O bloqueio de portas de mídia removível é adotado como **controle preventivo padrão**.

13.1 Política de uso

• Uso proibido por padrão.
• Exceções exigem autorização formal, previamente aprovada e registrada.
• O uso deve estar vinculado à necessidade de negócio, sendo restrito ao mínimo necessário.
• toda utilização deve ser rastreável e passível de auditoria.

13.2 Exceções

• Concedidas apenas quando indispensáveis e devidamente justificadas.
• vinculadas a processo formal, com definição de escopo, prazo e responsável.
• devem considerar análise de risco associada ao uso da mídia removível.
• devem possuir registro formal contendo: solicitante, justificativa, período e tipo de acesso concedido.

13.3 Cuidados obrigatórios

• Respeitar a classificação da informação;
• armazenar apenas o estritamente necessário (princípio da minimização);
• remover arquivos imediatamente após o uso autorizado;
• utilizar criptografia obrigatoriamente quando houver dados sensíveis ou pessoais;
• assegurar que os dados não sejam copiados, transferidos ou compartilhados fora dos meios autorizados;
• garantir que a mídia esteja protegida contra acesso não autorizado.

13.4 Solicitação

- Solicitação via Help Desk;
- Avaliação técnica;
- Liberação temporária;
- Revogação automática após uso.

13.5 Monitoramento

• Todos os desbloqueios, acessos e operações devem ser registrados em log;
• os registros devem conter identificação do usuário, data, horário e ação realizada;
• O uso de mídias removíveis deve ser monitorado continuamente;
• Auditorias periódicas verificam conformidade, uso adequado e revogação dos acessos;
• os registros devem ser mantidos como evidência auditável no âmbito do SGI..

13.6 Sanções

- O uso de mídias removíveis sem autorização formal ou em desacordo com esta política constitui incidente de segurança grave, sujeito a medidas disciplinares, administrativas e legais, de acordo com a gravidade.
- Tais ocorrências devem ser registradas, tratadas e analisadas conforme o processo de gestão de incidentes;

- Estão sujeitas a medidas disciplinares, administrativas e legais, conforme a gravidade e impacto;
- Casos envolvendo dados pessoais devem observar os requisitos da LGPD, incluindo avaliação de impacto e medidas cabíveis.

14 CONTROLES DE ACESSO

A Fenox Tecnologia estabelece controles formais e estruturados para garantir que o acesso físico e lógico aos seus ativos de informação, instalações e sistemas ocorra de forma **segura, individualizada, rastreável e proporcional ao risco**, em conformidade com os princípios de **menor privilégio**, **necessidade de uso** e **segregação de funções**.

Esses controles visam prevenir acessos não autorizados, reduzir riscos operacionais, proteger dados pessoais e assegurar evidências adequadas para auditorias internas e externas.

Todo acesso deve ser concedido, revisado e revogado por meio de processo formal, com registro obrigatório e evidência auditável no âmbito do Sistema de Gestão Integrado.

14.1 Acesso físico

O acesso físico às instalações da Fenox ocorre por **camadas independentes de controle**, reduzindo o risco de acesso indevido e garantindo rastreabilidade.

O acesso físico deve ser restrito a usuários autorizados, sendo obrigatória a manutenção de registros de entrada e saída contendo identificação, data, horário e finalidade, passíveis de auditoria.

14.1.1 A) Controle predial (recepção do edifício)

- Todos os colaboradores são cadastrados como pertencentes à unidade Fenox no sistema da recepção do prédio.
- O cadastro habilita:
- reconhecimento facial para entrada no edifício;
- liberação das catracas dos elevadores.
- O controle predial registra tentativas de acesso, entradas e saídas.

Os registros de acesso devem se mantidos conforme política de retenção definida, assegurando sua utilização como evidência em auditorias e investigações de incidentes

14.1.2 B) acesso à unidade fenox – 9º andar

- O acesso ao andar é controlado pelo sistema **ID Home**.
- O método preferencial é a **biometria digital**, garantindo unicidade do usuário.
- O uso de senha é tratado como **método transitório**, com plano de redução gradual, sob responsabilidade da Infraestrutura.
- Todos os acessos são registrados para fins de auditoria.

O uso de métodos de autenticação alternativos deve ser controlado, justificado e monitorado, sendo gradualmente eliminado quando não atender aos requisitos de segurança definidos.

14.1.3 C) sistema de alarme (panther)

- O sistema de alarme é operado apenas por colaboradores formalmente autorizados.
- As credenciais são individuais, restritas e revisadas periodicamente.
- O acionamento e desacionamento do alarme gera registro automático.

As permissões devem ser revisadas quando necessário, garantindo que apenas usuários autorizados mantenham acesso ao sistema.

14.1.4 D) visitantes e terceiros

- O acesso de visitantes depende de cadastro prévio na recepção.
- O acesso ao 9º andar é permitido apenas com acompanhamento de colaborador autorizado.
- Visitantes não possuem acesso autônomo às áreas internas nem aos sistemas.

Qualquer tentativa de acesso indevido, falha de autenticação ou anomalia deve ser comunicada imediatamente à Infraestrutura para avaliação e registro como evento de segurança.

O acesso de terceiros deve possuir registro formal contendo identificação, empresa, sendo vedado o acesso desacompanhado a áreas restritas.

14.2 Acesso lógico

O acesso lógico aos sistemas corporativos é concedido de forma **individual, controlada e proporcional às atribuições do usuário**.

Todos os acessos devem ser vinculados a identidades únicas, sendo vedado o uso de contas compartilhadas, exceto quando autorizado, controlado e rastreável.

14.2.1 Active directory (fenoxnet. local)

- Controle centralizado de autenticação.
- Políticas de senha com expiração, histórico e complexidade.

14.2.2 Sfile / repositórios de arquivos

- Controle por grupos de segurança.
- Permissões alinhadas à área e função.

As permissões devem ser revisadas, assegurando aderência à função e necessidade de negócio.

14.2.3 Sistema de gestão Fenox

- Perfis definidos conforme necessidade operacional.
- Acesso restrito a aplicações e registros pertinentes.
- Os acessos devem ser monitorados e registrados, garantindo rastreabilidade das operações realizadas.

14.2.4 Backoffice fenox

- Permissões concedidas conforme perfil funcional.
- O uso deve ser auditável, com registro de atividades relevantes para investigação de incidentes.

14.2.5 E-mail corporativo (microsoft 365)

- MFA habilitado.
- Gerenciamento centralizado pelo Admin Center.
- O compartilhamento de credenciais é expressamente proibido.

14.3 PRINCÍPIOS DE CONCESSÃO DE ACESSO

A concessão de acessos observa:

- menor privilégio;

- necessidade funcional;
- temporalidade quando aplicável.

Criação, alteração ou revogação de acessos ocorre mediante:

- solicitação formal do gestor;
- validação da Infraestrutura;
- registro para fins de rastreabilidade.

Perfis administrativos são limitados a usuários designados e sujeitos a revisão periódica.

Os acessos concedidos devem ser revisados , com base em função, necessidade e risco, sendo obrigatória a manutenção de evidências dessas revisões.

14.4 MONITORAMENTO E AUDITORIA

- Acessos físicos são registrados por:
- recepção;
- ID Home;
- sistema Panther.
- Acessos lógicos são monitorados por logs e controles sistêmicos.
- Revisões são realizadas sempre que:
- identificada mudança de risco;
- houver incidente;
- forem observadas oportunidades de melhoria.

Os registros de acesso devem conter identificação do usuário, data, horário e ação realizada, sendo mantidos conforme política de retenção e disponíveis para auditorias.

14.5 REVOGAÇÃO DE ACESSOS

Em desligamentos ou encerramento contratual:

- acessos físicos e lógicos são revogados imediatamente;
- dispositivos corporativos são recolhidos, resetados e avaliados;
- informações de trabalho são transferidas ao responsável designado.

A revogação deve ser registrada formalmente, assegurando rastreabilidade e evidência do encerramento dos acessos no app – podio sgpi.

14.6 Responsabilidades

- **Infraestrutura**: gestão técnica dos acessos.
- **Gestores**: solicitação e validação.
- **Colaboradores**: uso adequado das credenciais.
- **Diretoria**: aprovação de exceções.

O não cumprimento das diretrizes estabelecidas deve ser tratado como não conformidade ou incidente de segurança da informação, conforme aplicável, com registro, análise e tratamento no âmbito do SGI.

15 RESPONSABILIDADE DOS USUÁRIOS

Todos os usuários são corresponsáveis pela proteção das informações às quais têm acesso.

O uso dos ativos de informação deve observar as diretrizes de segurança, privacidade e conformidade estabelecidas, sendo obrigatório o registro e tratamento de desvios como incidente de segurança da informação ou não conformidade, conforme aplicável.

15.1 Senhas de acesso

- Senhas são pessoais e intransferíveis.
- Não devem ser registradas em meios inseguros.
- Senhas temporárias devem ser alteradas no primeiro acesso.
- Alteração imediata em caso de suspeita de comprometimento.
- É obrigatória a utilização de mecanismos que assegurem a confidencialidade das credenciais, sendo vedado qualquer compartilhamento ou reutilização indevida

15.2 Requisitos de qualidade

As senhas devem:

- possuir complexidade adequada;
- evitar padrões previsíveis;
- não conter dados pessoais.
- Devem atender aos requisitos definidos nas políticas de segurança da informação, incluindo critérios de tamanho, complexidade, histórico e expiração, quando aplicável.

15.3 Distribuição de senhas

- Entrega inicial ocorre por canal seguro.
- Em casos específicos, o coordenador pode apoiar o primeiro acesso, sem retenção de credenciais.
- Credenciais administrativas são sempre individuais.
- A distribuição deve ser registrada, assegurando rastreabilidade da entrega, identificação do usuário e evidência do processo.

15.4 Autenticação adicional

- MFA habilitado sempre que disponível.
- Bloqueio automático de estação configurado conforme perfil e risco.
- A autenticação adicional deve ser obrigatória para acessos a sistemas críticos, dados sensíveis ou acessos remotos, assegurando nível adequado de proteção.
- Utilizar os ativos de informação exclusivamente para finalidades autorizadas, sendo vedado qualquer uso indevido, acesso não autorizado ou tratamento de dados em desacordo com os requisitos estabelecidos.

15.5 Deveres do usuário

O usuário deve:

- proteger suas credenciais;
- reportar incidentes;
- não compartilhar acessos sob nenhuma circunstância.

16 USO DO CORREIO ELETRÔNICO

O correio eletrônico corporativo constitui ativo crítico da Fenox Tecnologia, sendo ferramenta oficial de comunicação e suporte às operações.

Seu uso deve ocorrer de forma segura, controlada, rastreável e alinhada às diretrizes de segurança da informação, privacidade e conformidade, assegurando a proteção dos dados, a integridade das comunicações e a manutenção de evidências para auditoria.

16.1 Propriedade e finalidade

- As contas de e-mail, conteúdos trafegados e registros associados são de propriedade da Fenox;
- O uso é estritamente profissional e vinculado às atividades da organização;
- os usuários são responsáveis pelas informações enviadas, recebidas e armazenadas;

• O uso deve observar os princípios de necessidade, confidencialidade e responsabilidade;
• O uso inadequado deve ser tratado como incidente de segurança ou não conformidade.

16.2 Diretrizes de uso

• As informações transmitidas devem respeitar a classificação definida pela organização;
• Informações confidenciais ou dados pessoais devem possuir tratamento adequado à sua criticidade;
• O envio deve ser limitado ao mínimo necessário (princípio da minimização);
• Dados pessoais devem ser tratados conforme a LGPD, com finalidade definida e controle de compartilhamento;
• O uso de anexos deve ser controlado, evitando exposição indevida de informações.

16.3 Proibições

• O ambiente de e-mail deve possuir filtros automáticos contra spam, phishing e malware;
• O acesso deve ser protegido por autenticação segura, incluindo MFA quando aplicável;
• O uso de criptografia deve ser aplicado para informações sensíveis ou confidenciais;
• as atividades devem ser registradas e monitoradas, assegurando rastreabilidade;
• Os acessos e eventos devem ser passíveis de auditoria.

16.4 Segurança

• Manter postura ética, profissional e alinhada às diretrizes da organização;
• Revisar destinatários, conteúdo e anexos antes do envio;
• Utilizar assinatura institucional e avisos legais definidos;
• Restringir o envio de informações a usuários autorizados;
• Reportar imediatamente e-mails suspeitos (phishing, malware ou engenharia social);
• Evitar envio desnecessário ou em massa de mensagens.

16.5 Exceções

• Envio de SPAM, correntes, pirâmides ou conteúdos indevidos;
• Uso de contas externas para envio ou resposta de comunicações corporativas sem autorização;
• Falsificação de identidade, remetente ou conteúdo;
• Compartilhamento indevido de informações confidenciais ou dados pessoais;
• Criação ou uso de contatos externos sem controle ou autorização;
• Utilização do e-mail para fins não autorizados ou ilegais.

16.6 Monitoramento, registro e auditoria

• As comunicações eletrônicas devem ser monitoradas conforme diretrizes de segurança;
• Logs de acesso, envio e recebimento devem vem ser mantidos;
• Os registros devem conter identificação do usuário, data, horário e ação realizada;
• As informações devem ser mantidas conforme política de retenção;
• Os registros devem estar disponíveis para auditorias e investigações.

16.7 Gestão de incidentes relacionados ao e-mail

• Eventos suspeitos devem ser tratados como incidentes de segurança da informação;
• devem ser registrados, classificados e analisados;
• devem possuir tratamento, evidência e rastreabilidade;
• Incidentes envolvendo dados pessoais devem seguir requisitos da LGPD.

16.8 Exceções

• Exceções devem ser solicitadas formalmente via sistema oficial;
• devem ser avaliadas quanto ao risco, justificativa e necessidade;

• devempossuir aprovação formal e prazo definido;
• devem ser registradas e monitoradas;
• ao término, devem ser automaticamente revogadas.

17 SOFTWARE EM ESTAÇÕES DE TRABALHO

As estações de trabalho são ativos corporativos críticos e estão sujeitas a controle contínuo, assegurando proteção, rastreabilidade e conformidade com os requisitos de segurança da informação, privacidade e governança.

Seu uso deve ocorrer exclusivamente para fins autorizados, sendo obrigatória a aplicação de controles técnicos e administrativos que garantam a integridade, confidencialidade e disponibilidade das informações.

17.1 Proteção das estações

- As estações devem possuir mecanismos de proteção ativos, incluindo antivírus, criptografia e bloqueio automático de sessão;
  • O bloqueio deve ocorrer automaticamente conforme perfil de risco e inatividade;
  • As estações devem estar inventariadas de forma individualizada, com identificação do responsável;
  • Deve ser aplicada política de mesa limpa e tela limpa, evitando exposição indevida de informações;
  • As configurações de segurança devem ser padronizadas e controladas pela área de Infraestrutura.

17.2 Uso de informações

- A utilização deve ocorrer exclusivamente em equipamentos corporativos homologados;
  • É proibido o uso de dispositivos pessoais para acesso, armazenamento ou tratamento de informações corporativas, salvo quando formalmente autorizado;
  • O uso das estações deve observar a classificação da informação e os requisitos de segurança e privacidade;
  • As informações devem ser acessadas e manipuladas apenas conforme necessidade de negócio.

17.3 Gestão de softwares

- Somente softwares homologados e autorizados podem ser instalados;
  • A instalação deve ocorrer mediante solicitação formal via sistema oficial;
  • Toda instalação, alteração ou remoção deve ser registrada e rastreável;
  • Deve haver monitoramento periódico das estações para identificação de softwares não autorizados;
  • Softwares não homologados devem ser removidos imediatamente;
  • Atualizações e correções de segurança devem ser aplicadas de forma controlada.

17.4 Direitos autorais

- Deve ser assegurado o cumprimento integral da legislação aplicável relacionada a direitos autorais e licenciamento de software;
  • É proibida a instalação ou uso de software ilegal ou sem licença válida;
  • A organização deve manter controle sobre licenças e evidências de conformidade.

17.5 Auditoria

- As estações de trabalho devem ser monitoradas quanto ao uso, integridade e conformidade;
  • Auditorias periódicas e não anunciadas devem ser realizadas;
  • devem ser mantidos registros e evidências das verificações realizadas;

• Os resultados devem ser utilizados para análise crítica e melhoria contínua do SGI;
• Eventos relevantes devem ser registrados para investigação de incidentes.

17.6 Sanções

- Violações devem ser tratadas como incidentes de segurança da informação;
  • devem ser registradas, analisadas e tratadas conforme o processo de gestão de incidentes;
  • Estão sujeitas a medidas disciplinares, administrativas e legais, conforme a gravidade;
  • Casos envolvendo dados pessoais devem observar os requisitos da LGPD.

18 UTILIZAÇÃO DE ELEMENTOS DE REDE

A rede corporativa é essencial à operação, à prestação de serviços e à segurança da informação, devendo ser utilizada de forma controlada, segura, rastreável e conforme os requisitos do Sistema de Gestão Integrado.

Seu uso deve assegurar a proteção contra acessos não autorizados, vazamentos de informação, indisponibilidade de serviços e riscos à privacidade dos dados tratados.

18.1 Conexão de dispositivos

- É proibida a conexão de dispositivos não autorizados à rede corporativa;
  • A conexão de qualquer ativo deve ser previamente validada e homologada pela área de Infraestrutura;
  • Todos os dispositivos conectados devem ser identificados, registrados e associados a um responsável;
  • A Infraestrutura é responsável pela gestão, controle e monitoramento dos dispositivos conectados;
  • Conexões não autorizadas devem ser tratadas como incidente de segurança da informação.

18.2 Armazenamento em rede

- A utilização de repositórios corporativos é obrigatória para armazenamento de informações;
  • Arquivos armazenados localmente não possuem garantia de backup e devem ser evitados;
  • O armazenamento deve respeitar a classificação da informação e os requisitos de segurança e privacidade;
  • A gestão de espaço deve ser controlada por área, conforme necessidade operacional;
  • Os dados devem ser protegidos contra acesso não autorizado, perda ou alteração indevida.

18.3 Uso adequado e conteúdo proibido

- É proibido o armazenamento ou tráfego de conteúdos pessoais, ilícitos ou não relacionados às atividades da organização;
  • É vedada a execução de softwares, serviços ou equipamentos que possam comprometer a segurança da rede;
  • O uso da rede deve estar alinhado às diretrizes de uso aceitável e classificação da informação;
  • Qualquer uso indevido deve ser tratado como incidente de segurança.

18.4 Controles técnicos de segurança

- A rede deve possuir controles técnicos ativos, incluindo firewalls, segmentação de rede e mecanismos de proteção;
  • O tráfego deve ser monitorado continuamente para identificação de comportamentos anômalos;
  • Logs e eventos de rede devem ser registrados, analisados e mantidos como evidência;
  • Os controles devem ser revisados periodicamente, considerando riscos e mudanças no ambiente;

• Medidas devem ser adotadas para prevenir acessos não autorizados e vazamento de informações.

18.5 Responsabilidades

18.5.1 • Infraestrutura:

– gestão, segurança, monitoramento e controle da rede;
– análise de eventos e resposta a incidentes;

18.5.2 • Colaboradores:

– uso adequado da rede corporativa;
– cumprimento das diretrizes estabelecidas;
– comunicação de eventos ou incidentes suspeitos;

O uso da rede deve ser monitorado e passível de auditoria, sendo obrigatória a manutenção de evidências que comprovem a aplicação dos controles estabelecidos.

19 TRABALHO REMOTO (HOME OFFICE)

A Fenox Tecnologia admite o trabalho remoto como modalidade excepcional e condicionada, aplicável exclusivamente a funções que não exijam presença física nas instalações da empresa. Essa modalidade não altera as responsabilidades do colaborador nem reduz os requisitos de segurança, confidencialidade, disponibilidade da informação e proteção de dados pessoais exigidos no ambiente corporativo presencial.

O trabalho remoto deve reproduzir, na medida do possível, o mesmo nível de controle, rastreabilidade e cuidado aplicado no escritório, especialmente no tratamento de informações institucionais, dados pessoais e dados regulados.

As atividades realizadas em regime remoto devem ser controladas, monitoradas e passíveis de auditoria, sendo obrigatória a manutenção de registros e evidências que comprovem a execução das atividades, os acessos realizados e o tratamento das informações.

19.1 Elegibilidade

O trabalho remoto poderá ser autorizado quando:

- as atividades do cargo não dependerem de acesso físico a ativos, documentos ou processos internos restritos;
  • houver viabilidade técnica e operacional para execução das atividades de forma segura;
  • for realizada avaliação de risco relacionada à segurança da informação, privacidade e continuidade das operações.

Colaboradores em período de integração ou em fase inicial de atuação permanecem, como regra, em regime presencial até que:

- compreendam os processos internos;
  • estejam aptos a operar com autonomia;
  • possam ser supervisionados adequadamente.

A autorização para trabalho remoto é sempre avaliada caso a caso, formalmente registrada e pode ser revogada a qualquer momento, conforme necessidade operacional ou de segurança.

19.2 Ferramentas e meios oficiais

Durante o trabalho remoto, somente ferramentas corporativas autorizadas devem ser utilizadas para execução das atividades e comunicação, incluindo:

- Podio: registro, acompanhamento e evidência de atividades, prazos e entregas;
  • Microsoft 365 (Outlook, Teams, SharePoint, OneDrive): comunicação interna, reuniões virtuais e gestão documental;
  • Sistemas corporativos web (Backoffice, Consultacorp, DashDETRAN): acesso mediante credenciais válidas e controles de autenticação;
  • Telefone e WhatsApp corporativo: comunicação externa com clientes e parceiros, observando as regras de uso aceitável e confidencialidade.

O uso de ferramentas pessoais ou plataformas externas não autorizadas não é permitido para tratamento de informações corporativas ou dados pessoais.

O uso das ferramentas deve ser registrado e monitorado, assegurando rastreabilidade das atividades e conformidade com os requisitos de segurança da informação e privacidade.

19.3 Ativos e equipamentos

- Equipamentos fornecidos pela Fenox devem ser registrados no Podio, com indicação clara do uso em trabalho remoto;
  • O colaborador é responsável pela guarda, integridade e uso adequado dos ativos recebidos;
  • Equipamentos pessoais não devem ser utilizados para atividades críticas, salvo autorização formal e controlada pela Infraestrutura;
  • Os ativos devem possuir controles de segurança ativos, incluindo autenticação, proteção contra ameaças, criptografia quando aplicável e rastreabilidade de uso.

19.4 Requisitos do ambiente remoto

O colaborador deve assegurar que:

- a conexão à internet seja estável e segura;
  • o ambiente físico impeça acesso de terceiros às informações corporativas;
  • telas, documentos e conversas não sejam expostos a familiares, visitantes ou pessoas não autorizadas;
  • chamadas e reuniões ocorram em local apropriado, evitando exposição de dados sensíveis.

O ambiente remoto deve reduzir riscos de exposição, vazamento ou acesso indevido às informações, sendo responsabilidade do colaborador assegurar condições adequadas de segurança.

19.5 Disponibilidade e supervisão

- O colaborador deve indicar sua disponibilidade no início da jornada;
  • Durante o expediente, deve manter-se acessível para reuniões, contatos e orientações;
  • A supervisão das atividades deve ocorrer de forma equivalente ao ambiente presencial, com acompanhamento por gestores e uso de registros operacionais;
  • As atividades devem ser registradas em sistemas corporativos, garantindo rastreabilidade, controle e evidência das entregas realizadas.

19.6 Segurança da informação e proteção de dados

Durante o trabalho remoto:

- acessos devem ocorrer exclusivamente por canais seguros e autenticados;
  • dispositivos devemutilizar senha forte, bloqueio automático de tela e proteção ativa contra ameaças;
  • informações corporativas e dados pessoais não devem ser armazenados em dispositivos

pessoais;
• o envio de informações deve respeitar os canais autorizados e a classificação da informação;
• práticas de mesa limpa e tela limpa devem ser mantidas mesmo fora do escritório;
• dados pessoais devem ser tratados exclusivamente para as finalidades autorizadas, sendo vedado qualquer uso indevido ou não autorizado, conforme a LGPD.

19.7 RESPONSABILIDADES

- Colaborador: cumprir horários, proteger os ativos, garantir a confidencialidade das informações e utilizar os recursos de forma adequada;
  • Infraestrutura: fornecer meios técnicos seguros, controle, suporte e monitoramento de acessos;
  • Gestores: validar a elegibilidade, acompanhar resultados e supervisionar adequadamente as atividades;

O não cumprimento das responsabilidades deve ser tratado como incidente de segurança da informação ou não conformidade, conforme aplicável, com registro, análise e tratamento no âmbito do SGI.

19.8 SANÇÕES

O descumprimento das diretrizes de trabalho remoto pode resultar em:

- advertências;
  • revogação da autorização para trabalho remoto;
  • bloqueio de acessos;
  • medidas disciplinares e legais, especialmente em casos de incidente de segurança ou vazamento de dados.

As ocorrências devem ser registradas, analisadas e tratadas conforme o processo de gestão de incidentes, assegurando rastreabilidade, identificação de causa e aplicação de ações corretivas.

20 ACESSOS PRIVILEGIADOS

A Fenox Tecnologia estabelece que acessos privilegiados representam alto impacto operacional e de segurança e, por isso, devem ser concedidos de forma restrita, justificada, temporária, controlada e plenamente rastreável.

O uso de privilégios elevados não é extensão do acesso comum e não deve ser tratado como prática rotineira.

Todos os acessos privilegiados devempossuir registro formal de concessão, uso, revisão e revogação, sendo passíveis de auditoria no âmbito do Sistema de Gestão Integrado.

20.1 DEFINIÇÃO

São considerados acessos privilegiados aqueles que permitem:

- instalar, remover ou alterar softwares;
  • modificar configurações de sistemas, redes ou estações;
  • criar, alterar ou excluir contas de usuários;
  • acessar dados e serviços críticos de forma ampliada;

Esses acessos devem ser classificados como de alto risco e tratados com controles reforçados.

20.2 CONCESSÃO DE ACESSOS

- O uso de privilégios administrativos locais requer justificativa formal, aprovação do gestor e validação da Infraestrutura;

• Perfis administrativos de domínio, rede, banco de dados ou aplicações críticas são atribuídos apenas a profissionais designados e autorizados;
• Acessos extraordinários devem ser temporários, com definição de prazo, escopo e responsável;
• Toda concessão deve ser registrada, assegurando rastreabilidade e evidência auditável;
• O acesso deve ser concedido com base no princípio do menor privilégio e necessidade de negócio.

20.3 SEGREGAÇÃO DE FUNÇÕES

Sempre que possível:

- atividades rotineiras devem ser realizadas com conta de usuário comum;
  • contas administrativas devem ser utilizadas exclusivamente para tarefas críticas e pontuais;
  • deve ser evitada a concentração de privilégios em um único usuário;

O uso de privilégios implica responsabilidade direta sobre as ações executadas, sendo todas passíveis de rastreamento.

20.4 PROIBIÇÕES

É expressamente vedado:

- alterar configurações sem autorização formal;
  • instalar softwares não homologados;
  • compartilhar credenciais privilegiadas;
  • manter privilégios ativos sem necessidade operacional;
  • utilizar acessos privilegiados para atividades não autorizadas ou fora do escopo definido.

20.5 MONITORAMENTO E AUDITORIA

- Atividades realizadas com acessos privilegiados devem ser registradas em logs detalhados;
  • Os registros devem conter identificação do usuário, data, horário e ação realizada;
  • A Infraestrutura realiza monitoramento contínuo e revisões periódicas dos acessos;
  • Auditorias verificam a adequação da concessão, uso e revogação dos privilégios;
  • Eventos suspeitos devem ser tratados como incidentes de segurança da informação.

21 ACESSOS LÓGICOS

O acesso lógico aos sistemas, aplicações e à rede corporativa da Fenox é estruturado de forma centralizada, padronizada e controlada, assegurando que toda autenticação, autorização e uso de recursos digitais seja individual, rastreável e compatível com a função exercida.

A utilização do Active Directory (AD) como núcleo de identidade garante uniformidade de controles, redução de acessos indevidos, segregação funcional e capacidade de auditoria contínua, mitigando riscos de uso não autorizado, vazamento de informações e falhas de governança.

Todos os acessos devem ser concedidos, revisados e revogados por meio de processo formal, com registro obrigatório e evidência auditável.

21.1 PROVISIONAMENTO DE ACESSOS

- Cada colaborador recebe **credenciais únicas e intransferíveis**, criadas exclusivamente pela Infraestrutura, garantindo unicidade de identidade digital.
- O provisionamento ocorre **somente após solicitação formal do coordenador da área**, assegurando alinhamento entre necessidade operacional e privilégio concedido.
- O ingresso no domínio **fenoxnet. local** estabelece o vínculo técnico entre usuário, estação e ambiente corporativo, permitindo controle centralizado de políticas, autenticação e auditoria.

- Os acessos são organizados por **grupos de segurança**, garantindo que permissões sejam atribuídas por função e não de forma individualizada e arbitrária.

Essa abordagem reduz riscos de concessões excessivas e facilita revisões periódicas.

21.2 SEGREGAÇÃO DE PERFIS

- O princípio do **menor privilégio** é adotado como base de todo provisionamento.
- Perfis administrativos representam risco elevado e, por isso, são **limitados, justificados e monitorados**.
- A segregação impede que usuários comuns executem ações capazes de comprometer sistemas, dados ou continuidade operacional.
- O uso de perfis elevados deve ser justificado e rastreável.

21.3 GESTÃO DO CICLO DE VIDA DE IDENTIDADES

A gestão de identidades é tratada como processo contínuo e não como evento isolado:

- **Criação:** ocorre apenas mediante solicitação formal e aprovação hierárquica.
- **Manutenção:** revisões semestrais garantem aderência entre função atual e acessos concedidos, prevenindo acúmulo indevido de permissões.
- **Revogação:** desligamentos ou mudanças de função geram revogação imediata, evitando contas órfãs e riscos residuais.

Essa prática sustenta rastreabilidade e reduz exposição indevida. Todos os eventos devem ser registrados, assegurando rastreabilidade e evidência auditável.

21.4 CONTROLES TÉCNICOS

- Políticas de senha aplicadas via AD garantem **complexidade, expiração e histórico**, reduzindo riscos de comprometimento.
- A autenticação multifator adiciona uma **camada adicional de proteção**, especialmente para acessos remotos e serviços críticos.
- Logs de autenticação permitem **detecção, investigação e resposta a eventos suspeitos**, fortalecendo a capacidade de reação a incidentes.
- O acesso remoto segue os mesmos critérios de segurança aplicados internamente, evitando exceções técnicas que fragilizem o ambiente.
- Os registros devem ser mantidos conforme política de retenção e disponíveis para auditoria.

21.5 RESPONSABILIDADES

- **Infraestrutura:** atua como guardiã do controle de identidades e acessos.
- **Gestores:** validam continuamente a necessidade de acessos concedidos.
- **Colaboradores:** respondem pelo uso correto de suas credenciais, reconhecendo que todo acesso é pessoal e auditável.

- O não cumprimento deve ser tratado como incidente ou não conformidade.

21.6 SANÇÕES

Qualquer tentativa de burlar controles, compartilhar credenciais ou acessar recursos não autorizados será tratada como violação grave de segurança da informação.

As ocorrências devem ser registradas, analisadas e tratadas conforme o processo de gestão de incidentes, podendo resultar em medidas disciplinares e legais.

21.7 PADRÃO PARA CRIAÇÃO DE LOGINS

A padronização de logins:

- evita ambiguidades;
- facilita auditorias;
- assegura consistência entre sistemas.

A preservação de logins antigos garante histórico técnico e evidência de rastreabilidade, sendo vedada a reutilização indevida de identidades.

22 ACESSOS FÍSICOS

O controle de acessos físicos é tratado como extensão direta da segurança da informação, reconhecendo que a proteção lógica é ineficaz sem controle físico adequado.

O objetivo é impedir acesso indevido, preservar ativos críticos, proteger dados pessoais e assegurar responsabilização clara, rastreabilidade e evidência auditável.

Todos os acessos físicos devem ser autorizados, registrados, monitorados e passíveis de auditoria, com manutenção de evidências conforme diretrizes do Sistema de Gestão Integrado.

22.1 ENTRADA DE TERCEIROS E VISITANTES

A autorização formal via grupo corporativo cria:

- registro explícito da decisão;
- identificação do responsável;
- evidência auditável de autorização.

Esse modelo elimina liberações informais e dependência de decisões verbais, assegurando controle formal e rastreabilidade.

22.2 AGENDAMENTO

O pré-cadastro garante previsibilidade e evita acessos improvisados.

- Todo acesso deve ser previamente registrado;
  • O agendamento deve conter identificação do visitante, empresa, responsável interno, data, horário e finalidade;
  • A ausência de cadastro prévio impede o acesso, salvo exceções formalmente autorizadas e registradas;

Os registros devem ser mantidos como evidência para auditoria.

22.3 RECEPÇÃO

O acompanhamento obrigatório de visitantes, prestadores e fornecedores tem por finalidade:

- **restringir a circulação** às áreas estritamente necessárias à atividade autorizada;
- **reduzir risco de acesso indevido** a informações, estações de trabalho, documentos e ativos físicos;
- **evitar exposição acidental** de dados pessoais e informações confidenciais por observação, fotografia, coleta ou manuseio não autorizado;
- **assegurar rastreabilidade** do responsável pela recepção e acompanhamento durante toda a permanência;

- **garantir encerramento controlado** do acesso, com confirmação de saída e devolução de itens temporariamente entregues (quando aplicável).
- O visitante não deve possuir acesso autônomo às instalações ou ativos da organização.

22.4 Finalidade

A sistemática tem como finalidade assegurar que os acessos sejam **autorizados, rastreáveis e auditáveis**, garantindo:

- **controle contínuo** sobre concessão, uso e revogação de acessos;
- **responsabilização objetiva** por meio da identificação inequívoca do solicitante, aprovador e usuário;
- **prevenção de acessos indevidos** e redução de permissões excessivas, por aplicação de perfis e grupos;
- **capacidade de verificação e investigação**, suportada por registros de autenticação e alterações de permissões, quando aplicável;
- **conformidade com requisitos internos e legais**, incluindo proteção de dados pessoais, limitando o acesso ao estritamente necessário.
- limitação do acesso ao estritamente necessário, conforme princípio do menor privilégio aplicado ao ambiente físico.

Se você quiser manter em **uma frase só**, robusta:

“A sistemática assegura que todo acesso seja concedido, utilizado e revogado de forma autorizada, rastreável e auditável, permitindo responsabilização objetiva, prevenção de acesso indevido e verificação por registros e evidências formais.”

23 COLABORADORES DESLIGADOS

A gestão de desligamento de colaboradores é tratada como processo crítico de segurança da informação, com foco na eliminação imediata de acessos, preservação da integridade dos ativos e manutenção da rastreabilidade.

O bloqueio imediato elimina riscos de:

- uso indevido pós-desligamento;
- acesso residual a sistemas;
- vazamento intencional ou acidental. **Bloqueio imediato (desligamento / término de contrato)**
  O bloqueio imediato elimina riscos de:
- **uso indevido pós-desligamento**, mantendo a integridade das credenciais e evitando continuidade de acesso fora de vínculo;
- **acesso residual a sistemas**, prevenindo permanência de permissões em AD/M365, aplicações internas e plataformas corporativas;
- **vazamento intencional ou acidental**, reduzindo exposição de dados pessoais, credenciais, documentos e informações operacionais;
- **alterações não autorizadas**, evitando exclusões, cópias, mudanças de configuração e movimentações de dados após o desligamento;
- **quebra de rastreabilidade**, preservando trilhas de auditoria e permitindo reconstrução de eventos quando necessário.

23.1 CONTROLES DE SEGURANÇA FÍSICA E OPERACIONAL

23.1.1 CFTV

O monitoramento contínuo:

- **desencoraja acessos indevidos**, por efeito dissuasório e visibilidade do controle;
- **fornece evidência objetiva em caso de incidente**, apoiando análise de eventos, horários e fluxos de entrada/saída;
- **apoia investigações internas e auditorias**, permitindo correlação com logs de sistemas e registros de visitantes;
- **sustenta resposta a incidentes**, com recuperação controlada das imagens mediante justificativa e necessidade;
- **reforça proteção de dados pessoais**, limitando acesso às imagens a pessoas autorizadas e mantendo retenção compatível com finalidade e necessidade.

23.1.2 ACOMPANHAMENTO DE TERCEIROS

A responsabilização do acompanhante impede delegação difusa de riscos ao assegurar:

- **ponto único de controle** durante a permanência do terceiro;
- **orientação e restrição de acesso**, evitando circulação em áreas não autorizadas e contato com ativos/informações;
- **registro de responsabilidade**, vinculando a autorização e a supervisão a um colaborador identificado;
- **controle de interação com sistemas e documentos**, reduzindo exposição acidental de dados pessoais e informações confidenciais;
- **encerramento formal**, com confirmação de saída e retirada de acessos temporários/credenciais de visita quando aplicável.

23.1.3 ACESSO AO CPD

O CPD é tratado como área crítica, exigindo controle reforçado, registro e acompanhamento formal, pois concentra ativos essenciais à operação e à proteção da informação. Assim:

- **o acesso é restrito por necessidade**, limitado a pessoas autorizadas e a atividades justificadas;
- **toda entrada deve ser rastreável**, com registro de data/hora, finalidade, responsável e presença de acompanhamento quando aplicável;
- **intervenções técnicas** convêm **gerar evidência**, como checklist de atividade, registro de manutenção e referência ao chamado/ação correspondente;
- **terceiros entram somente acompanhados**, com supervisão contínua e limitação de escopo;
- **medidas de proteção operacional são preservadas**, evitando alteração de configuração, conexões indevidas e manuseio não autorizado de equipamentos e mídias.

23.2 DISPOSITIVOS PERMITIDOS NA REDE

A rede corporativa é considerada **ativo crítico**, e qualquer dispositivo conectado passa a integrar o perímetro de risco.

• Apenas dispositivos homologados e autorizados podem ser conectados;
• Todos os dispositivos devem ser identificados, registrados e monitorados;
• A conexão indevida deve ser tratada como incidente de segurança;

A limitação a dispositivos homologados:

- reduz superfície de ataque;
- evita introdução de vulnerabilidades;
- mantém governança técnica do ambiente.

23.3 LIMITAÇÃO DE ACESSO

O controle centralizado via firewall e mecanismos de segurança permite:

- aplicação uniforme de políticas;
- bloqueio preventivo de categorias de risco;
- monitoramento contínuo do tráfigo.
- Registro de eventos para auditoria e investigação.

23.4 USO NÃO AUTORIZADO

A proibição protege a rede contra:

- Execução de malware;
- exfiltração de dados;
- uso indevido de banda e recursos computacionais.
- Acesso não autorizado a sistemas ou informações.
- Qualquer desvio deve ser tratado como incidente de segurança da informação.

23.5 PENALIDADES

Violações devem ser tratadas como incidentes formais, assegurando rastreabilidade, análise e responsabilização.

O processo deve garantir que:

- **ocorrências sejam registradas em canal oficial**, com identificação do evento, data/hora, origem, evidências disponíveis e classificação preliminar (ex.: acesso indevido, tentativa, compartilhamento de credencial, bypass de controle);

- **a contenção seja imediata quando aplicável**, incluindo bloqueio/revogação de acessos, reset de credenciais, isolamento de equipamento e suspensão temporária de permissões até avaliação técnica;

- **a apuração tenha base objetiva**, mediante correlação de registros (AD/M365, aplicações, rede, CFTV, controle de visitantes e registros de chamados/ações) e preservação de evidências;

- **haja avaliação de impacto**, incluindo risco operacional, continuidade, confidencialidade/integridade e exposição de dados pessoais, com direcionamento para ações corretivas e preventivas;

- **responsabilidades sejam atribuídas de forma clara**, com registro de envolvidos, aprovadores, responsáveis pela análise e responsáveis por ações de correção, evitando ambiguidade;

- **medidas administrativas sejam aplicadas de forma proporcional**, conforme gravidade, recorrência e risco, podendo incluir advertência formal, restrição de acesso, requalificação obrigatória e outras medidas internas previstas;

- **comunicações obrigatórias sejam acionadas quando necessárias**, especialmente em cenários com potencial violação de dados pessoais, seguindo o fluxo interno e requisitos legais aplicáveis;

- **a eficácia seja verificada**, confirmando que o controle foi restabelecido, o risco mitigado e que não permaneçam acessos residuais ou vulnerabilidades relacionadas.

24 USO DE DISPOSITIVOS PESSOAIS

O uso de dispositivos pessoais no ambiente corporativo é tratado como exceção controlada, reconhecendo necessidades operacionais específicas sem comprometer a segurança da informação, a proteção de dados pessoais e a governança dos ativos.

A autorização formal para uso de dispositivos pessoais:

- transfere responsabilidade ao usuário;
- mantém controle institucional;
- evita normalização de exceções.
- O uso não autorizado de dispositivos pessoais é expressamente proibido.Backup, Storage e Restauração

As rotinas de backup são estruturadas para:

- garantir continuidade;
- minimizar perda de dados;
- permitir recuperação testada e comprovada.

A validação mensal transforma backup de “promessa” em **capacidade real**.

24.1 AUTORIZAÇÃO E CONTROLE

• O uso de dispositivos pessoais depende de autorização formal prévia;
• A solicitação deve conter justificativa, finalidade, escopo e prazo;
• A autorização deve ser registrada e passível de auditoria;
• A liberação deve considerar análise de risco à segurança da informação e privacidade;
• O acesso concedido deve ser limitado ao mínimo necessário.

24.2 REQUISITOS DE SEGURANÇA

Dispositivos pessoais autorizados devem atender aos seguintes requisitos mínimos:

• utilização de autenticação segura (senha ou biometria);
• bloqueio automático de tela;
• proteção contra malware e ameaças;
• sistema operacional atualizado;
• criptografia quando aplicável.

Dispositivos que não atendam aos requisitos não devem ser utilizados.

24.3 USO E TRATAMENTO DA INFORMAÇÃO

• O acesso deve ocorrer exclusivamente por meios e sistemas corporativos autorizados;
• O armazenamento local de informações corporativas deve ser evitado;
• Dados pessoais e informações confidenciais devem ser tratados conforme sua classificação;
• O compartilhamento de informações deve ocorrer apenas por canais oficiais;
• É vedada a cópia, transferência ou retenção indevida de dados.

24.4 MONITORAMENTO E CONTROLE

• O uso de dispositivos pessoais deve ser monitorado quando conectado ao ambiente corporativo;
• Acessos e atividades devem ser rastreáveis;
• Eventos suspeitos devem ser registrados e tratados como incidente de segurança;
• A autorização pode ser revogada a qualquer momento, conforme risco identificado.

24.5 RESPONSABILIDADES

• Colaborador: garantir uso seguro, proteção do dispositivo e cumprimento das diretrizes;
• Infraestrutura: avaliar, autorizar, controlar e monitorar o uso;
• Gestores: validar a necessidade e acompanhar o uso autorizado.

O não cumprimento das diretrizes deve ser tratado como incidente de segurança da informação ou não conformidade.

24.6 SANÇÕES

• O uso não autorizado ou inadequado de dispositivos pessoais constitui violação das diretrizes de segurança;
• As ocorrências devem ser registradas e tratadas conforme o processo de gestão de incidentes;
• Podem resultar em bloqueio de acesso, revogação de autorização e medidas disciplinares;
• Casos envolvendo dados pessoais devem observar os requisitos da LGPD.

25 ATIVOS TECNOLÓGICOS

Os ativos tecnológicos da Fenox Tecnologia sustentam a operação dos serviços críticos de negócio, o tratamento de dados pessoais, a continuidade operacional e a integridade das informações sob custódia da organização.

Sua gestão considera critérios de disponibilidade, resiliência, integridade, segurança lógica e física, bem como rastreabilidade e capacidade de recuperação em cenários de falha ou incidente.

Todos os ativos devem ser monitorados, controlados e passíveis de auditoria, com manutenção de evidências conforme diretrizes do Sistema de Gestão Integrado.

25.1 Servidores

Os servidores são configurados com mecanismos de tolerância a falhas, incluindo fontes redundantes e volumes em RAID 6.

Esses mecanismos:

• reduzem o risco de indisponibilidade por falhas físicas isoladas;
• asseguram continuidade dos serviços essenciais;
• evitam pontos únicos de falha.

Os serviços críticos (Active Directory, DNS e DHCP) operam em ambiente replicado, garantindo:

• continuidade da autenticação;
• resolução de nomes;
• distribuição de endereços IP;

As atualizações de sistemas operacionais e serviços:

• seguem planejamento prévio;
• possuem análise de impacto;
• são aplicadas de forma controlada;

As atividades devem ser registradas e rastreáveis.

25.2 Storages

A Fenox mantém três storages corporativos (FSTG01, FSTG02 e FSTG03) em ambiente controlado:

• FSTG01 – 8 discos de 18 TB (RAID 1);
• FSTG02 – 24 discos de 18 TB (RAID 6);
• FSTG03 – 12 discos de 18 TB (RAID 6, SO em RAID 1).

Esses ativos armazenam:

• dados operacionais;
• registros técnicos;
• evidências de serviço;
• informações de clientes;

25.3 CONFIGURAÇÕES

• RAID 1: alta confiabilidade com espelhamento;
• RAID 6: tolerância a falha de até dois discos;

A definição considera criticidade, volume e tempo de recuperação.

25.4 Topologia de rede

A arquitetura é estruturada para garantir segurança, redundância e disponibilidade.

25.4.1 COMPONENTES

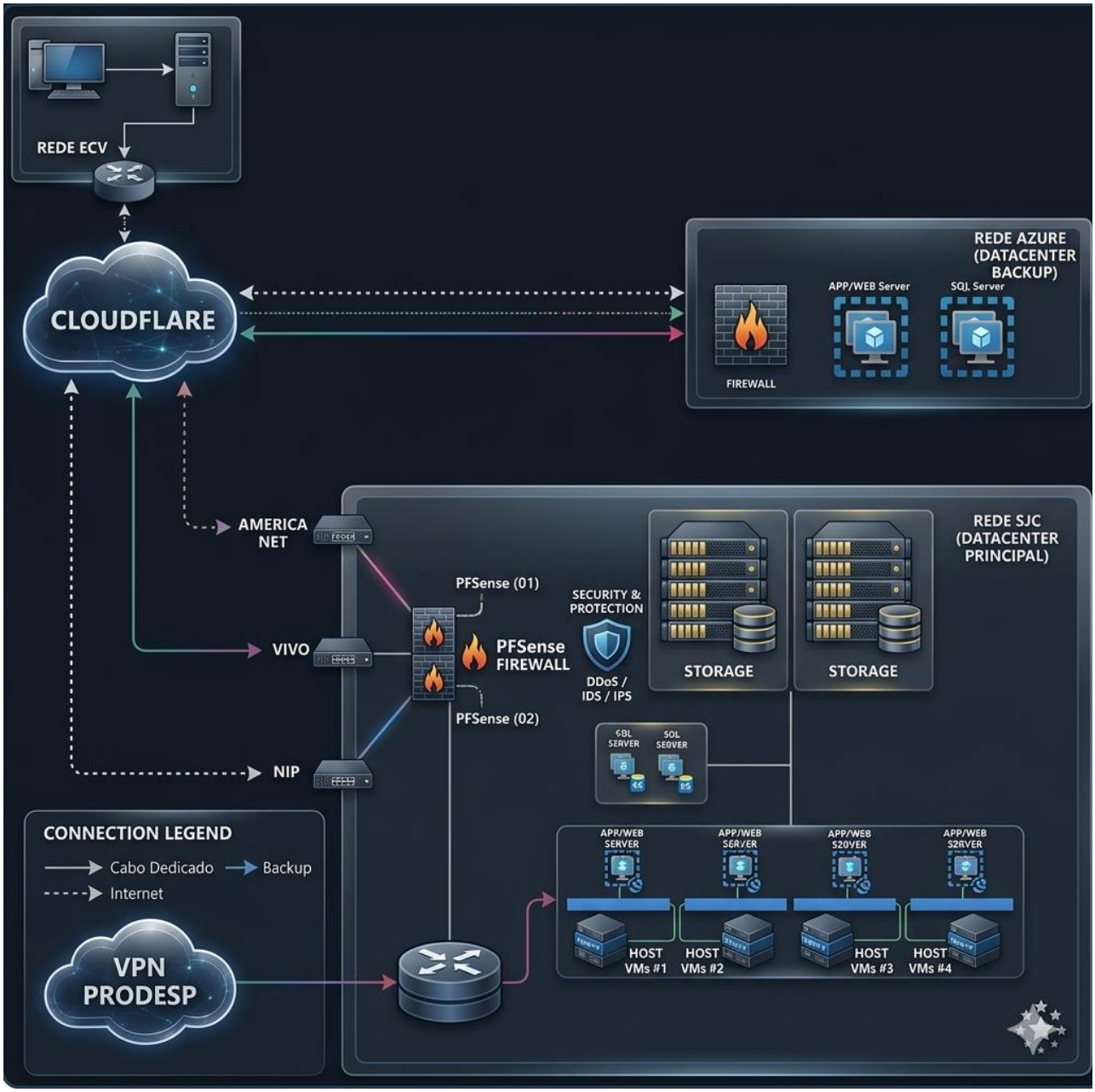
• Data Center Principal (SJC):
  – servidores, banco de dados e storages;
  – firewalls pfSense redundantes;
  – múltiplos links de internet;

• Ambiente de Backup (Azure):
  – contingência em nuvem;
  – continuidade operacional;

• Integrações externas:
  – Cloudflare (proteção e balanceamento);
  – VPN Prodesp (acesso seguro governamental);

• Rede ECV:
  – ambiente segregado;
  – controle de acesso e isolamento;

A arquitetura evita pontos únicos de falha e protege dados em trânsito.



25.5 Links de comunicação e conectividade

A conectividade é composta por múltiplos provedores:

• Americanet:
  – VPN Prodesp (200 Mbps);
  – link corporativo (700 Mbps);

• NipBR:
  – link dedicado (200 Mbps);

• Vivo:
  – VPN Prodesp (200 Mbps);

O firewall realiza failover automático, garantindo continuidade dos serviços.

25.6 Cloudflare e gocache

A Fenox utiliza:

• CDN;
• WAF;
• DNS gerenciado;
• proteção contra DDoS;

Em caso de falha, a GoCache atua como redundância.

25.7 Contingência – microsoft azure

Em falhas do ambiente principal:

• tráfego redirecionado via Cloudflare/GoCache;
• domínio reconfigurado;
• banco passa de Read-Only para Read-Write;

A ativação é controlada e registrada.

25.8 Roteadores

• equipamentos gerenciados pelos provedores;
• suporte conforme SLA contratado;

25.9 Nobreaks e energia

• nobreaks garantem operação contínua;
• autonomia de até 120 minutos;
• atendem requisitos regulatórios;

Monitoramento e manutenção são realizados periodicamente.

25.10 Manutenção de equipamentos críticos

• Gerador: manutenção trimestral;
• Nobreaks: manutenção semestral;
• Ar-condicionado CPD: manutenção anual;

25.11 Controle e registro

• Manutenções identificadas por monitoramento ou rotina;
• Registros realizados no Podio;
• Evidências obrigatórias;

25.12 Objetivo

Minimizar riscos técnicos, assegurando:

• continuidade dos serviços;
• proteção das informações;
• estabilidade operacional;

25.13 Monitoramento contínuo

Os ambientes são monitorados continuamente, garantindo:

• disponibilidade;
• integridade;
• segurança da informação;

25.14 Sincronização de tempo

• uso de NTP;
• padronização de logs;
• consistência de registros;

25.15 Monitoramento de logs

• monitoramento diário de acessos;
• relatórios mensais consolidados;
• rastreabilidade de usuários e ações;

25.16 Monitoramento de infraestrutura

Sistema Nagios monitora:

• servidores;
• serviços críticos;
• discos;
• memória;

25.17 Atualizações de segurança

• verificação contínua de patches e firmware;
• aplicação controlada;
• redução de vulnerabilidades;

25.18 Controle de acesso remoto

A organização pode restringir acessos em caso de:

• descumprimento da política;
• uso indevido;
• risco identificado;

25.19 Gestão de servidores (ecv)

Responsabilidades:

• especificação técnica;
• homologação;
• instalação e configuração;
• gestão de banco de dados;

Atualizações:

• críticas: automáticas;
• demais: avaliadas e programadas;

26 ATIVOS DE COMUNICAÇÃO

A Fenox Tecnologia mantém inventário, controle e gestão dos ativos de comunicação utilizados para suportar a conectividade, a segurança perimetral e o tráfego de dados corporativos, assegurando disponibilidade, integridade, confidencialidade e proteção das informações tratadas.

A gestão desses ativos considera critérios de criticidade, risco, continuidade operacional e rastreabilidade, sendo todos passíveis de monitoramento e auditoria no âmbito do Sistema de Gestão Integrado.

Ativo	Identificação / Responsabilidade
Firewalls	pfSense (01 e 02) operando em alta disponibilidade (HA), responsáveis pelo controle de tráfego, segmentação de rede e aplicação de regras de segurança. Cloudflare e GoCache atuam como camadas adicionais de proteção externa, mitigando riscos de ataque e indisponibilidade. Dell EdgeRouter é utilizado para regras específicas de comunicação no CPD.
Switches	Equipamentos das marcas Dell e Cisco, responsáveis pela distribuição e segmentação do tráfego interno, garantindo desempenho, controle e isolamento lógico entre ambientes.
Servidores	Servidores Dell, utilizados para hospedar serviços corporativos críticos, com configuração voltada à resiliência, controle de acesso e rastreabilidade.
Roteadores	Equipamentos de diversas marcas, de propriedade e responsabilidade das operadoras contratadas (Americanet, Vivo, NipBR), garantindo conectividade externa conforme SLA contratado.

26.1 Gestão e controle

• A gestão dos ativos é responsabilidade da Infraestrutura;
• Todos os ativos devem ser identificados, registrados e associados a responsáveis;
• As configurações devem ser controladas e padronizadas;
• Alterações devem seguir processo formal e rastreável;
• Os ativos devem ser classificados conforme criticidade e impacto.

26.2 Monitoramento e segurança

• Os ativos devem ser monitorados continuamente;
• Logs e eventos devem ser registrados e analisados;
• Controles de segurança devem ser aplicados conforme risco;
• Eventos suspeitos devem ser tratados como incidentes de segurança;
• Os registros devem ser mantidos como evidência auditável.

26.3 Manutenção e continuidade

• Os ativos devem possuir manutenção preventiva e corretiva;
• A disponibilidade deve ser garantida por redundância e failover;
• Planos de contingência devem ser aplicáveis quando necessário;
• Intervenções devem ser registradas e controladas;

26.4 Responsabilidades

• Infraestrutura: gestão, configuração, monitoramento e segurança;
• Gestores: validação de necessidades e priorização;
• Colaboradores: uso adequado dos recursos de comunicação;

O não cumprimento deve ser tratado como incidente ou não conformidade.

27 ATENDIMENTO A USUÁRIOS

A Fenox Tecnologia adota processo formal, padronizado e rastreável para atendimento a usuários internos, assegurando qualidade, agilidade, controle operacional e histórico auditável das interações realizadas.

O processo está alinhado às práticas de gestão de serviços, permitindo controle de demanda, mensuração de desempenho e melhoria contínua.

27.1 Fluxo de atendimento

Processo	Interveniente	Entrada	Saída
Abertura de chamado	Suporte Técnico	Demanda recebida via SURI ou diretamente no WhatsApp corporativo	Chamado registrado no BackOffice, com identificação do solicitante, data e escopo da demanda
Validação e Distribuição	Suporte Técnico	Chamado aberto	Chamado direcionado ao atendente responsável, conforme tipo e prioridade
Resolução	Suporte Técnico	Chamado em atendimento	Solução aplicada, com comunicação clara ao usuário demandante
Encerramento	Suporte Técnico	Atendimento realizado	Registro das atividades executadas e encerramento formal do chamado no BackOffice, preferencialmente via SURI
Métricas	BackOffice	Medição das demandas	Relatórios de chamados, tempo médio de atendimento, resolução e indicadores de SLA

Esse fluxo garante **visibilidade do atendimento**, **responsabilização técnica** e **base objetiva para análise de desempenho**.

27.2 Diretrizes

- O **BackOffice** é o sistema oficial e obrigatório de gestão de chamados da Fenox, sendo a fonte única de registro e evidência;
- A **SURI** atua como canal inicial de comunicação e automação, integrada ao WhatsApp e ao BackOffice, garantindo registro automático sempre que possível;
- Quando o fluxo automatizado não ocorrer, o registro manual no BackOffice é obrigatório;
- As métricas extraídas subsidiam auditorias internas, análises críticas e ações de melhoria contínua, assegurando controle sobre qualidade, prazos e recorrência de demandas.

27.3 Controle e rastreabilidade

- Todos os atendimentos devem ser registrados em sistema oficial;
  • Os registros devem conter identificação, data, descrição e solução;
  • O histórico deve ser mantido para auditoria e análise;
  • O processo deve permitir rastreabilidade ponta a ponta;

27.4 Gestão de nível de serviço (sla)

- Os atendimentos devem seguir critérios de prioridade e criticidade;
  • O cumprimento de SLA deve ser monitorado continuamente;
  • Indicadores devem ser analisados periodicamente;
  • Desvios devem gerar ações corretivas;

27.5 Monitoramento e melhoria contínua

- Os dados de atendimento devem ser utilizados para melhoria contínua;
  • Relatórios devem suportar análise crítica do SGI;
  • O processo deve ser revisado conforme necessidade;
  • O desempenho deve ser acompanhado por indicadores definidos;

27.6 Responsabilidades

- Suporte Técnico: execução e registro dos atendimentos;
  • Infraestrutura: suporte técnico especializado;
  • Gestores: priorização e acompanhamento;
  • Usuários: abertura adequada de chamados e fornecimento de informações;

27.7 Sanções e tratamento de desvios

- Desvios devem ser registrados e tratados como não conformidade ou incidente;
  • devem em possuir análise de causa e ações corretivas;
  •devem ser mantidas evidências do tratamento;

28 PRIVACIDADE E PROTEÇÃO DE DADOS

A Fenox Tecnologia assegura que o tratamento de dados pessoais ocorra de forma lícita, transparente, controlada e segura, respeitando os direitos dos titulares e preservando a confiança de clientes, parceiros e colaboradores.

O tratamento de dados pessoais é conduzido em conformidade com a legislação aplicável, diretrizes internas e requisitos de segurança da informação, garantindo rastreabilidade, proteção e evidência das operações realizadas.

28.1 Responsabilidades

- Clientes internos e externos com acesso físico às instalações são informados, desde a contratação, sobre suas responsabilidades quanto à segurança e privacidade das informações;
  • O uso de dados pessoais ocorre em conformidade com esta Política, diretrizes internas e legislação aplicável;
  • Cada colaborador atua como corresponsável pela proteção dos dados aos quais possui acesso, respondendo pelo uso adequado e autorizado;

28.2 Controles de acesso

- O acesso a sistemas, painéis administrativos e bases contendo dados pessoais ocorre mediante autenticação individual e controlada;
  • As permissões são concedidas conforme função, perfil e necessidade operacional, observando o princípio do menor privilégio;
  • Acessos são registrados, monitorados e passíveis de auditoria;
  • Acessos indevidos, excessivos ou não autorizados são tratados como incidentes de segurança da informação;

28.3 Tratamento e retenção de dados

- Dados pessoais e sensíveis são coletados e tratados para finalidades legítimas, específicas e previamente definidas;
  • O armazenamento ocorre em ambientes controlados, com segregação de acesso e aplicação de controles técnicos de proteção;
  • A retenção é limitada ao período necessário para atendimento das finalidades, podendo ser estendida em casos de obrigação legal, regulatória ou contratual;
  • Após o término do período de retenção, a eliminação ocorre de forma segura e rastreável;

• Quando aplicável, os dados são anonimizados, eliminando a possibilidade de identificação do titular;

28.4 Princípios de privacidade

O tratamento de dados pessoais na Fenox é orientado pelos princípios de:

- finalidade;
  • necessidade;
  • transparência;
  • segurança;
  • responsabilização e prestação de contas;

Esses princípios orientam as decisões técnicas, operacionais e administrativas relacionadas ao tratamento de dados pessoais, assegurando conformidade, controle e governança da informação.

29 SANÇÕES E VIOLAÇÃO DE SEGURANÇA

Qualquer violação desta Política ou das normas internas de Segurança da Informação é tratada como incidente formal, com registro, análise, rastreabilidade e responsabilização no âmbito do Sistema de Gestão Integrado.

As ocorrências são avaliadas quanto à natureza, impacto, recorrência e risco à segurança da informação, à continuidade dos serviços e à proteção de dados pessoais.

29.1 Tratamento de violações

• As violações são registradas em sistema oficial, contendo identificação do evento, data, origem e evidências disponíveis;
• A análise considera impacto operacional, risco à informação e eventual exposição de dados pessoais;
• A apuração ocorre com base em evidências, incluindo registros de sistemas, acessos, rede e controles físicos, quando aplicável;
• As ações adotadas incluem contenção, correção e prevenção de recorrência;
• Todas as etapas são documentadas, assegurando rastreabilidade e suporte a auditorias;

29.2 Medidas aplicáveis

As sanções podem incluir, conforme gravidade e contexto:

• medidas administrativas e disciplinares;
• suspensão ou revogação de acessos;
• restrição temporária de atividades ou funções;
• desligamento;
• responsabilização civil ou criminal, quando aplicável;

A aplicação ocorre de forma proporcional à gravidade, recorrência e impacto da ocorrência.

29.3 Proteção de dados pessoais

• Ocorrências envolvendo dados pessoais são tratadas conforme requisitos da LGPD;
• A avaliação considera risco aos titulares e impacto à organização;
• As comunicações obrigatórias são realizadas quando aplicável;
• As ações adotadas buscam mitigar impactos e prevenir recorrência;

29.4 Evidência e auditoria

- Todos os registros relacionados às violações são mantidos como evidência;
- As informações permanecem disponíveis para auditorias internas e externas;
- Os dados suportam análises críticas e melhoria contínua do SGI;