Política de Segurança da Informação

Código: PL-TI-01

Classificação da Informação: Pública.

Tipo de Documento: Política**.**

Departamento Responsável: Tecnologia da Informação.

1 OBJETIVO

A Política de Segurança da Informação define diretrizes para proteger os ativos de informação da Elea Data Centers, reduzir riscos e assegurar conformidade com requisitos legais e normativos.

A política assegura:

- Confidencialidade;
- Integridade;
- Disponibilidade.

A Elea Data Centers está comprometida com a melhoria contínua dos controles e desta Política, por meio de monitoramento, análises críticas e auditorias periódicas. Esta Política é revisada, no mínimo, anualmente ou sempre que houver mudanças relevantes no ambiente de negócios, tecnológico ou regulatório.

2 APLICAÇÃO

Esta política se aplica a todos que tenham acesso às informações da organização, incluindo colaboradores, prestadores de serviço, fornecedores e visitantes.

Todos devem:

- Cumprir as diretrizes estabelecidas;
- Proteger os ativos de informação;
- Reportar incidentes de segurança.

3 DEFINIÇÕES

Para os efeitos desta Política, aplicam-se os seguintes termos e definições:

- **Áreas críticas:** Dependências da Elea Data Centers ou de seus clientes onde esteja situado um ativo de informação relacionado a informações críticas para os negócios da empresa ou de seus clientes.
- **Ameaça:** Causa potencial de um incidente indesejado que pode resultar em danos a um sistema ou organização.

- **Análise de riscos:** Uso sistemático de informações para identificar fontes e estimar o risco.
- **Avaliação de riscos:** Processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.
- **Ataque:** Tentativa para destruir, expor, alterar, desabilitar, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um ativo.
- **Ativo:** Qualquer componente, recurso ou conjunto destes aplicáveis para a preservação da confidencialidade, integridade e disponibilidade de dados e informações (hardware, software, infraestrutura, pessoas com seus conhecimentos etc.).
- **Ativo da informação:** Conhecimento ou dados que tenham valor para a empresa.
- **Comunicação de risco:** Troca ou compartilhamento de informações sobre riscos entre o tomador de decisões e outras partes interessadas.
- **Confiabilidade:** Característica de comportamento consistente e resultados desejados.
- **Confidencialidade:** Característica de informação não está disponível nem pode ser revelada a indivíduos, entidades ou processos não autorizados.

4 DOCUMENTOS E REFERÊNCIA

N/A

5 PAPÉIS E RESPONSABILIDADES

Alta Direção

Responsável por garantir que a segurança da informação esteja alinhada à estratégia da empresa, disponibilizando recursos, promovendo cultura de segurança e assegurando a melhoria contínua do SGI.

Área de Governança e Qualidade

Responsável por manter e monitorar a política, além de promover auditorias.

Área de TI

Responsável pela execução dos controles técnicos, incluindo gestão de acessos, segurança de sistemas, backups, monitoramento e proteção contra ameaças.

Colaboradores e prestadores de serviço

Responsáveis por utilizar corretamente os recursos, proteger as informações e reportar qualquer situação que represente risco à segurança.

Encarregado de Dados Pessoais (DPO)

Responsável por assegurar a conformidade com a legislação de proteção de dados pessoais aplicável, incluindo a Lei Geral de Proteção de Dados (LGPD). Compete ao Encarregado:

- Atuar como ponto de contato entre a organização, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- Orientar colaboradores e terceiros quanto às práticas de proteção de dados pessoais;
- Apoiar na implementação e monitoramento de controles relacionados à privacidade;
- Acompanhar e orientar o tratamento de incidentes que envolvam dados pessoais;
- Assegurar que os processos de tratamento de dados estejam em conformidade com os requisitos legais e normativos aplicáveis;
- Promover a cultura de proteção de dados pessoais na organização.

6 DIRETRIZES GERAIS DE SEGURANÇA

A Elea Data Centers estabelece e mantém controles tecnológicos para proteger os ativos de informação contra ameaças internas e externas, assegurando a confidencialidade, integridade e disponibilidade das informações, com base na análise de riscos e na criticidade dos ativos e processos de negócio.

São adotadas soluções de proteção contra códigos maliciosos, incluindo antivírus e antimalware com atualização automática e monitoramento contínuo, bem como práticas de gestão de vulnerabilidades, contemplando verificações periódicas e aplicação de correções de segurança conforme o nível de risco identificado.

Os sistemas, aplicações e dispositivos são mantidos atualizados de forma contínua, visando reduzir exposições a ameaças conhecidas. As informações críticas são protegidas por meio de rotinas de backup, armazenadas em ambientes seguros e testadas periodicamente para garantir sua recuperação quando necessário.

Os sistemas possuem mecanismos de registro e monitoramento de eventos, assegurando rastreabilidade e suporte a auditorias e investigações, com proteção adequada contra alterações indevidas. O acesso aos sistemas é controlado por meio de autenticação,

credenciais individuais e gestão de privilégios, garantindo que apenas usuários autorizados tenham acesso às informações.

São utilizados mecanismos de criptografia para proteção de dados sensíveis, tanto em trânsito quanto, quando aplicável, em repouso. A infraestrutura de rede é protegida por controles como firewalls, segregação de redes e monitoramento contínuo, visando garantir a segurança das comunicações e acessos.

O uso de serviços em nuvem segue critérios de segurança definidos, incluindo avaliação de riscos, controle de acessos e monitoramento das atividades. Os sistemas e dispositivos são configurados conforme padrões seguros, com controle de alterações e revisões periódicas, assegurando a manutenção de um ambiente tecnológico seguro e alinhado às melhores práticas.

7 GESTÃO DE PESSOAS

A Elea Data Centers reconhece que as pessoas são parte fundamental para a proteção das informações e para a eficácia do Sistema de Gestão de Segurança da Informação. Nesse contexto, todos os colaboradores, prestadores de serviço e terceiros devem atuar de forma consciente e responsável, compreendendo seu papel na preservação da confidencialidade, integridade e disponibilidade das informações.

A organização promove continuamente ações de treinamento e conscientização, visando assegurar que todos estejam aptos a identificar riscos, adotar boas práticas de segurança e agir de forma preventiva no desempenho de suas atividades. É responsabilidade de cada indivíduo proteger as informações às quais tem acesso, utilizando os recursos corporativos de forma adequada e em conformidade com as diretrizes estabelecidas.

No ambiente de trabalho, devem ser observadas as práticas de mesa limpa e tela limpa, com o objetivo de evitar a exposição indevida de informações. Documentos físicos contendo informações sensíveis não devem permanecer visíveis sobre mesas ou estações de trabalho quando não estiverem em uso, devendo ser armazenados em locais seguros. Da mesma forma, equipamentos e estações de trabalho devem ser bloqueados sempre que o usuário se ausentar, ainda que por curtos períodos, prevenindo acessos não autorizados.

Adicionalmente, espera-se de todos os colaboradores um comportamento íntegro, ético e alinhado às normas internas e à legislação vigente. Isso inclui o uso responsável das

informações, a não divulgação de dados confidenciais sem autorização, o respeito às políticas corporativas e a comunicação imediata de qualquer situação que represente risco à segurança da informação ou à organização. O descumprimento dessas diretrizes poderá comprometer a segurança dos ativos de informação e sujeitar o responsável às medidas administrativas e legais cabíveis.

8 GESTÃO DA INFRAESTRUTURA FÍSICA

A Elea Data Centers estabelece e mantém controles rigorosos de segurança física com o objetivo de proteger seus ambientes, ativos de informação e infraestrutura crítica contra acessos não autorizados, danos, interferências e ameaças físicas ou ambientais. Considerando a natureza dos serviços prestados, que envolvem operações de Data Center e serviços de Colocation, a proteção do ambiente físico é tratada como elemento essencial para a continuidade dos negócios e a confiança de seus clientes.

As instalações são projetadas e operadas com base em princípios de segurança em camadas, incluindo a definição de perímetros físicos protegidos, controle de acesso restrito e monitoramento contínuo. O acesso às áreas críticas, como salas de servidores, data halls e ambientes de suporte, é permitido apenas a pessoas devidamente autorizadas, mediante mecanismos de autenticação e registro, garantindo rastreabilidade das entradas e saídas.

A organização adota controles como sistemas de vigilância por vídeo (CFTV), equipes de segurança, barreiras físicas e procedimentos formais para gestão de visitantes, assegurando que qualquer acesso seja previamente autorizado, acompanhado quando necessário e devidamente registrado.

Adicionalmente, os ambientes são protegidos contra ameaças físicas e ambientais, incluindo falhas elétricas, incêndios, variações de temperatura, umidade e outros eventos que possam comprometer a operação. Para isso, são utilizados sistemas redundantes de energia (como UPS e geradores), controle de climatização, detecção e combate a incêndio, bem como rotinas de manutenção preventiva e corretiva dos equipamentos críticos.

A Elea Data Centers também garante a segregação adequada de ambientes, separando áreas operacionais, administrativas e de clientes, de forma a reduzir riscos e assegurar níveis apropriados de proteção conforme a criticidade dos ativos.

9 GESTÃO DE INCIDENTES

Todos os incidentes de segurança devem ser imediatamente reportados através do ServiceNow e tratados conforme processo definido.

A gestão de incidentes visa:

- Reduzir impactos;
- Corrigir falhas;
- Evitar recorrência.

Os incidentes são registrados e analisados para melhoria contínua.

10 EXCEÇÕES

Exceções e casos omissos a esta política serão tratados conforme os procedimentos específicos aplicáveis a cada um dos tópicos abordados, podendo, quando necessário, ser definidos pela área responsável pela gestão desta política.

11 VIOLAÇÕES E SANÇÕES

A violação às políticas, normas ou procedimentos da Elea Data Centers, bem como a não aderência à Política de Segurança da Informação, à Política de Privacidade ou ao Manual de Ética e Conduta da Elea Data Centers poderão acarretar sanções ou medidas disciplinares conforme descritos através da Política de Sanção Disciplinar.

12 ANEXOS

N/A

13 REGISTROS

Identificação	Classificação	Proteção	Local de Armazenamento	Recuperação	Tempo mínimo de retenção

N/A	N/A	N/A	N/A	N/A	N/A

14 HISTÓRICO DE ALTERAÇÕES

DATA	REVISÃO	ELABORADOR	APROVADOR	DESCRIÇÃO
04/10/2024	6.0	LAÍS GEDRAITS	SEGURANÇA DA INFORMAÇÃO, TI, JURÍDICO, RECURSOS HUMANOS E ALTA DIREÇÃO	ATUALIZAÇÃO NA DISPOSIÇÃO DAS INFORMAÇÕES NO DOCUMENTO, ALÉM DA CLASSIFICAÇÃO DA INFORMAÇÃO.
25/08/2025	6.1	LAÍS GEDRAITS	SGI E ALTA DIREÇÃO	ATUALIZAÇÃO DO DOCUMENTO, COM A INCLUSÃO DO CANAL DE COMUNICAÇÃO EHS, E NOVAS LEIS COMO A ANPD E CLT.
23/06/2026	7.0	BIANCA GUGLIELMELLI	WILLIAM RAIMUNDO	REVISÃO GERAL DO DOCUMENTO.