SANTA MARIA
Energia que transforma

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Código:	SGSI-POL-001
Versão:	1.0
Data da versão:	12/11/2024
Criado por:	Yotta Tech
Aprovado por:	Conselho de Administração
Nível de confidencialidade:	Pública

Histórico de alterações

Data	Versão	Criado por	Descrição da alteração
12/11/2024	1.0	Yotta Tech	Esboço básico do documento

Histórico de revisões

Data	Revisão	Revisado por	Descrição da revisão

Sumário

1. Finalidade, escopo e usuários

A finalidade desta Política de alto nível é definir a finalidade, a direção, os princípios e as regras básicas de gestão da segurança da informação e segurança cibernética na Empresa Luz e Força Santa Maria S.A.

Os usuários deste documento são colaboradores da Empresa Luz e Força Santa Maria S.A, assim como as partes externas relevantes.

2. Documentos de referência

- Norma ISO/IEC 27001:2022, cláusulas 5.1, 5.2, 5.3 e A.5.1, A.5.2
- Norma IS 3.1.2 O/IEC 27002:2022
- Resolução Normativa ANEEL Nº 964, de 14 de dezembro de 2021

3. Terminologia básica de segurança da informação

Ativos – qualquer coisa que tenha valor para a organização. No contexto da segurança da informação, dois tipos de ativos podem ser distinguidos:

- Ativos primários:
  - Informação;
  - Processos de negócios e atividades;
- Ativos de suporte (dos quais os ativos primários dependem) de todos os tipos:
  - *Hardware;*
  - *Software;*
  - Rede
  - Pessoal
  - Local
  - Estrutura da organização

Confidencialidade – características das informações que estão disponíveis somente para pessoas autorizadas ou sistemas.

Integridade - características das informações que somente são alteradas por pessoas da forma permitida.

Disponibilidade - características das informações que somente pode ser acessada por pessoas autorizadas quando for necessário.

Segurança da informação - Refere-se à proteção de informações contra acesso não autorizado, divulgação, alteração e destruição. Abrange medidas técnicas e administrativas para garantir a confidencialidade, integridade e disponibilidade das informações.

Segurança Cibernética - Foca na proteção de sistemas, redes e dados no contexto do ciberespaço, que inclui a internet e outras redes de comunicação. Envolve a defesa contra ataques cibernéticos como malware, phishing, ataques DDoS, e outras ameaças digitais e inclui práticas como firewalls, sistemas de detecção de intrusão, e atualizações de segurança.

Privacidade - é um conceito que se refere ao direito de uma pessoa ou grupo de pessoas de manterem suas informações pessoais e atividades fora do alcance de terceiros não autorizados. É a capacidade de controlar o acesso e a divulgação de informações pessoais.

Sistema de gestão da segurança da informação (SGSI) - É um conjunto de políticas, procedimentos e tecnologias utilizadas para gerenciar e proteger as informações de uma organização.

Incidente cibernético - é qualquer evento ou conjunto de eventos indesejados e inesperados que comprometem a segurança da informação ou das operações em um ambiente cibernético. O ambiente cibernético, também conhecido como ciberespaço, inclui a internet, redes privadas, sistemas de comunicação e toda a infraestrutura digital que permite o armazenamento, processamento e transmissão de dados. Isso abrange computadores, dispositivos móveis, servidores, sistemas de informação e redes de comunicação.

4. Gerenciando a segurança da informação

4.1. Objetivos da segurança da informação e medição

Os objetivos gerais para a segurança da informação são os seguintes:

- Atender as exigências legais e regulatórias relacionadas à segurança da informação, cibernética e de privacidade;
- Estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI) para estabelecer capacidades operacionais em:
    - Governança
    - Gestão de ativos
    - Proteção da informação
    - Segurança em recursos humanos
    - Segurança física
    - Segurança de sistemas e rede
    - Segurança de aplicação
    - Configuração segura
    - Gestão de identidade e acesso
    - Gestão de ameaças e vulnerabilidades
    - Continuidade
    - Segurança nas relações com fornecedores
    - Leis e *Compliance*
    - Gestão de eventos de segurança da informação
    - Garantia de segurança da informação

  - Estabelecer um programa de treinamento e ações de conscientização em segurança da informação, segurança cibernética e privacidade;
  - Estabelecer um plano de ação e resposta à incidentes de segurança da informação e segurança cibernética;
- Garantir a eficácia dos controles de segurança da informação, segurança cibernética e de privacidade para assegurar a confidencialidade, integridade e disponibilidade dos ativos bem como a privacidade;
- Avaliar o nível de maturidade em segurança cibernética anualmente conforme o Programa de Auditoria Interna e Externa da Empresa Luz e Força Santa Maria S.A.

Para alcançar os objetivos definidos para a Segurança da Informação e Privacidade, é determinado o Planejamento Anual dos Objetivos de Segurança da Informação, Segurança Cibernética e de Privacidade, este é acompanhado periodicamente nas reuniões de análises críticas de Segurança da Informação e Privacidade, onde são verificados os índices de atendimento e níveis de maturidade conforme indicadores definidos.

4.2. Requisitos de segurança da informação

A Alta Administração está comprometida com uma gestão efetiva da Segurança da Informação na Empresa Luz e Força Santa Maria S.A. Desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização.

Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação as necessidades da Empresa Luz e Força Santa Maria S.A.

Esta Política deve estar em conformidade com os requisitos legais e regulamentares vigentes e aplicáveis à organização na área de segurança da informação, bem como com as obrigações contratuais.

4.3. Controles da segurança da informação e segurança cibernética

Medidas técnicas e administrativas

Medidas técnicas e administrativas devem ser definidas para mitigação de riscos. Através do Sistema de Gestão de Segurança da Informação (SGSI), são estabelecidos processos que definem controles para classificação e tratamento de ativos conforme sua relevância, além de procedimentos e controles para reduzir a vulnerabilidade a incidentes, atender aos objetivos de segurança da informação e segurança cibernética, e gerenciar incidentes.

Documentação e avaliação

A relação de informações documentadas do SGSI é registrada e mantida atualizada através do documento Lista Mestra do SGSI. A metodologia para avaliação e tratamento de riscos de segurança da informação e segurança cibernética define a abordagem de riscos adotada pela Empresa Luz e Força Santa Maria S.A. As medidas técnicas implementadas para garantir a segurança das informações críticas são registradas e mantidas atualizadas através do documento Inventário de Medidas Técnicas.

Os controles de tratamento de riscos de segurança da informação contidos no Anexo A da ISO 27001:2022, aplicáveis ao SGSI, estão declarados e justificados no documento Declaração de Aplicabilidade.

Políticas, instruções normativas e procedimentos

Através do SGSI, seus requisitos e controles, das medidas técnicas e administrativas, a Empresa Luz e Força Santa Maria S.A estabelece políticas, instruções normativas, procedimentos, processos e controles com foco em garantir a segurança da informação e segurança cibernética. Isso inclui:

Segurança dos ativos: Classificação conforme relevância e criticidade, conforme a Norma de Classificação da Informação, que estabelece diretrizes para classificação, rotulagem e tratamento dos ativos.

Gestão de incidentes de segurança: Inclui preparação, identificação, categorização, priorização, contenção e erradicação, recuperação, coleta e preservação de evidências, lições aprendidas, comunicação e equipe de resposta a incidentes, conforme estabelecido no Plano de Ação e Resposta a Incidentes.

Continuidade de negócios: O Plano de Recuperação de Desastres inclui identificação de processos críticos, desenvolvimento de estratégias de recuperação e realização de testes regulares para assegurar a eficácia das medidas implementadas visando garantir a resiliência operacional e a rápida recuperação em caso de incidentes significativos.

Avaliação de eficácia

A eficácia dos controles é avaliada através do acompanhamento contínuo dos objetivos de segurança da informação.

4.4. Responsabilidades

As responsabilidades básicas para o SGSI são:

- Conselho de Administração
  - Aprovar as políticas de segurança da informação e segurança cibernética
  - Atribuir responsabilidade e autoridade para assegurar que o sistema de gestão da segurança da informação está em conformidade com os requisitos da Norma ISO/IEC 27001 vigente;
  - Atribuir responsabilidade e autoridade à Alta Direção para relatar sobre o desempenho do sistema de gestão da segurança da informação ao Conselho de Administração.

- A Alta Direção deve:
  - Aprovar demais documentos derivados do Sistema de Gestão de Segurança da Informação (SGSI);

- Atribuir responsabilidade e autoridade às Gerências para relatar sobre o desempenho do sistema de gestão da segurança da informação para a Alta Direção;
- Assegurar que os recursos necessários para a gestão da segurança da informação estão disponíveis;
- Comunicar a importância de uma gestão eficaz da segurança da informação e da conformidade com os requisitos de gestão da segurança da informação;

- O Gerente de TI deve:
  - Garantir que a gestão da segurança da informação seja realizada em conformidade com esta Política e possua todos os recursos necessários.
  - Gerenciar e reportar sobre o desempenho da segurança da informação;
  - Implementar em conjunto com o RH um programa de Treinamento e Conscientização sobre segurança da informação para os colaboradores e todas as pessoas que possam impactar a segurança da informação.

- O DPO deve:
  - Garantir que a gestão de privacidade seja realizada em conformidade com esta Política e possua todos os recursos necessários.
  - Gerenciar e reportar sobre o desempenho de privacidade;
  - Reportar ao Gerente de TI sobre quaisquer preocupações relacionadas à segurança da informação e cibernética;
  - Implementar em conjunto com o RH um programa de Treinamento e Conscientização sobre privacidade para os colaboradores e todas as pessoas que possam impactar a privacidade.

- A Comissão de Segurança da Informação (CSI) deve:
  - Apoiar em reuniões de análise crítica da gestão da segurança da informação com a finalidade de auxiliar na verificação da adequabilidade e a eficácia dos controles de implementados;
  - Sinalizar possíveis impactos dos controles na área operacional;
  - Apoiar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente da Empresa Luz e Força Santa Maria S.A;
  - Apoiar na integração dos controles de segurança da informação com os processos do negócio;
  - Analisar a aplicação de sanções e punições desta política, bem como demais normas e procedimentos de segurança.

- A equipe de TI deve:
  - Propor metodologias, processos e iniciativas que visem à segurança da informação;
  - Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para a Empresa Luz e Força Santa Maria S.A;
  - Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes;

- Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;
- Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação;
- Habilitar trilha de auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes em transações críticas. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.
- Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos nesta política e pelas normas de segurança da informação complementares.
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Empresa Luz e Força Santa Maria S.A.

- Gestores de Pessoas e/ou Processos devem:
  - Ter postura exemplar em relação à segurança da informação e privacidade, servindo como modelo de conduta para os colaboradores sob a sua gestão;
  - Verificar se os colaboradores sob sua gestão, na fase de contratação e de formalização dos contratos individuais de trabalho e de prestação de serviços foram informados desta política e se foi coletado o aceite.
  - Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta política de segurança da informação.

- As equipes envolvidas no gerenciamento de Projetos devem:
  - Apoiar na verificação de requisitos de segurança da informação e privacidade desde a concepção dos projetos na Empresa Luz e Força Santa Maria S.A;
  - Reportar preocupações e fragilidades relacionadas a questões de segurança da informação e privacidade identificadas em projetos da Empresa Luz e Força Santa Maria S.A.

- Os usuários da Informação devem:
  - Ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança da Empresa Luz e Força Santa Maria S.A;
  - Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política de Segurança da Informação, e das normas e procedimentos de Segurança da Informação ou, quando pertinente, a Comissão de Segurança da Informação;
  - Comunicar a área de Tecnologia e Segurança da Informação qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da Empresa Luz e Força Santa Maria S.A;

- Assinar o Termo de Aceite formalizando a ciência e o aceite integral das disposições da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;
- Responder pela inobservância da Política de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.

- A proteção da integridade, disponibilidade e confidencialidade é responsabilidade do proprietário e do custodiante de cada ativo.
- Todos os incidentes e as fragilidades de segurança devem ser reportados a área de Tecnologia e Segurança da Informação que definirá quais informações relativas à segurança da informação serão comunicadas para qual parte interessada internamente e externamente, por quem e quando.

4.5. Comunicação da política

Esta política deve ser comunicada para todos os colaboradores da Empresa Luz e Força Santa Maria S.A, bem como para todas as partes externas apropriadas.

4.6. Sanções e Punições

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades previstas conforme os níveis estabelecidos na Matriz de Responsabilidade.

5. Suporte para a implementação do SGSI

Deste modo, a Alta Administração da Empresa Luz e Força Santa Maria S.A declara que a implementação da Gestão da Segurança da Informação e seu contínuo aprimoramento serão suportados pelos recursos apropriados para alcançar todos os objetivos definidos nesta Política, assim como para atender todos os requisitos identificados.

6. Validade e gestão de documentos

Este documento é válido a partir de sua aprovação.

O proprietário deste documento é o Gerente de TI, que deve verificar e, se necessário, atualizar o documento anualmente.