POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Âmbito e Objetivo

A presente Política de Segurança da Informação ("PSI") tem como objetivo estabelecer cultura que assegure a segurança das informações da **FUNFER FUNDIÇÃO DE FERRO LIMITADA** ("FUNFER").

2. Glossário

Colaborador: Pessoa física que presta serviço para a FUNFER e possui vínculo empregatício.

Prestador de Serviço: Pessoa física ou jurídica que presta serviço de qualquer natureza à FUNFER.

Fornecedor: Pessoa jurídica que fornece insumos de qualquer natureza, sejam eles serviços ou matérias-primas os quais são necessários para a FUNFER realizar suas atividades.

Usuário: Colaboradores ou prestadores de serviços, indiferente do vínculo a que estejam submetidos, como outros indivíduos ou organizações devidamente autorizadas a utilizar qualquer ativo ou informação da FUNFER para o desempenho de suas atividades profissionais.

Ativo: Bens (patrimônios) ou equivalentes, tangíveis ou intangíveis, os quais tenham valor para a FUNFER.

Ameaça: Potencial causa de incidente.

Incidente: Evento ou conjunto de eventos indesejados de segurança da informação que tenham possibilidade significativa de afetar as operações ou ameaçar as informações ou ativos da FUNFER.

Evento: Acontecimento que acarrete mudança do estado atual de um processo.

Risco: Probabilidade da ocorrência de um evento indesejado para a FUNFER, o qual pode afetar o cumprimento de seus objetivos.

Vulnerabilidade: Fragilidade que, caso materializada, pode gerar danos à organização.

Segurança da Informação: Conjunto de ações que visam a preservar e garantir a disponibilidade, confidencialidade e integridade das informações pertencentes e sob a responsabilidade da FUNFER, assim, mitigando os riscos e probabilidades de dano.

DPO (*Data Protection Officer*): é o encarregado de dados, conforme definição da LGPD. Pessoal responsável pela deliberação sobre fluxos, mudanças ou respostas a incidentes, dentre outros com relação aos tratamentos de dados pessoais dentro da FUNFER

Rua Benedito Gonçalves, nº. 1801, Jardim Floramar, Divinópolis/MG
Funfer Fundição de Ferro
www.funfer.com.br
(37) 3512-4900

3. Atribuições e responsabilidades

Diretoria Executiva

A Diretoria Executiva ("Diretoria") deve se comprometer em estabelecer normas, procedimentos, atividades de treinamento e conscientização que incentivem a execução das atividades descritas nessa PSI por parte dos usuários, auxiliando na disseminação e na revisão dos documentos.

Departamento de Tecnologia da Informação

A área de Tecnologia da Informação ("TI") é responsável por armazenar e auxiliar na atualização das políticas que corroboram para a manutenção do sistema de segurança da informação da FUNFER. Assim, a TI deve prover ambiente e infraestrutura seguros e compatíveis com suas diretrizes, devendo estar atenta para:

- Estabelecimento de mecanismos que identifiquem e divulguem alertas sobre novos tipos de ameaças e métodos de segurança de informações;
- Definição de diretrizes para a realização de inventário dos ativos da FUNFER que estejam associadas com informações;
- Acompanhamento dos projetos da FUNFER, assegurando que as áreas estão se resguardando e aplicando as diretrizes dessa PSI;
- Apoiar o DPO na implementação de mecanismos para garantir os direitos dos titulares de dados;
- Monitorar e implementar medidas de Segurança da Informação proporcionais aos riscos gerados pelo tratamento de dados pessoais e em linha com a expectativa de proteção dos titulares de dados pessoais, garantindo a integridade, disponibilidade e confidencialidade destas informações;
- Atualizar-se a fim de garantir que as técnicas mais avançadas e alinhadas com o mercado estejam sendo utilizadas e sugerir mudanças no que tange a segurança dos dados preventivamente e proativamente;
- Realizar avaliação de proteção de dados pessoais nos sistemas da FUNFER em caso de alterações nas práticas de gerenciamento e proteção de dados pessoais;
- Analisar violações e vazamentos de dados pessoais bem como efetuar a coleta de evidências técnicas para demonstração dos incidentes e se necessário, efetuar a interface com o departamento jurídico para endereçamento correto da violação/vazamento de dados;
- Responsabilizar-se pelo uso adequado de dados pessoais em suas atividades;

- Avaliar a proteção de dados nos sistemas da Empresa no caso de alterações nas práticas de gerenciamento e proteção de dados da FUNFER;
- Oferecer treinamentos específicos aos colaboradores da empresa a fim de evitar erros humanos relacionados ao TI, como por exemplo esclarecimentos sobre Spam, Phishing, compartilhamento de senhas e outras medidas que possam gerar vulnerabilidades nos sistemas;
- Facilitar a execução dos processos de:

  g.1. *Privacy by Default*: Avaliar as práticas de coleta e retenção de dados inibindo o processamento de dados excessivo;

  g.2. *Privacy by Design*: Considerar controles de privacidade e proteção de dados na implementação de novas tecnologias;

  g.3. *Data Security*: Avaliar práticas de proteção de dados com base em classificações de dados estabelecidas.
- Realizar *reports* e interações constantes ao DPO sobre questões relacionadas à Segurança da Informação.
- Monitorar contratações e manutenção de terceiros e/ou softwares de terceiros que possam representar riscos de vazamento e tratamento irregular de dados pessoais;
- Homologar internamente hardwares externos que estão autorizados a serem utilizados nas máquinas do FUNFER (tais como, porém, não restritos a *pendrives* pessoais, HDs externos pessoais, e outros).

Demais áreas

Os responsáveis por cada área devem ter postura exemplar em relação à segurança da informação e cumprimento das diretrizes descritas nessa PSI.

As áreas devem divulgar e cumprir as diretrizes estabelecidas nessa PSI, reforçando quais ativos e atividades referentes à segurança das informações são de responsabilidade de cada usuário, desde sua contratação. Deve-se ainda, considerar diretrizes de segregação de função, com os níveis de autorização claramente documentados e definidos.

Todo e qualquer projeto que ocorra nas áreas internas da FUNFER, independentemente de sua complexidade, deve levar em consideração as diretrizes citadas nessa PSI, atentando-se para os riscos envolvidos em seu desenvolvimento.

Rua Benedito Gonçalves, nº. 1801, Jardim Floramar, Divinópolis/MG
Funfer Fundição de Ferro
www.funfer.com.br
(37) 3512-4900

Usuários multiplicadores

Devem ler, compreender e seguir integralmente os termos da PSI, bem como as demais normas e procedimentos correlatos.

4. Diretrizes

A política de Segurança da Informação da FUNFER reforça o seu compromisso com a proteção dos dados e das informações que estão sob sua responsabilidade.

O uso de informações e ferramentas de TI devem ser feitos sempre de forma ética, transparente e em respeito aos princípios da confidencialidade e finalidade no uso de informações.

5. Gestão de Riscos e Incidentes

A área de TI é responsável pela gestão de riscos e incidentes acerca de ativos, a qual visa prevenir a indisponibilidade das atividades e, no caso de alguma interrupção, possuir ações estruturadas para restabelecer sua normalidade o mais rapidamente possível, consequentemente, minimizando os prejuízos às áreas de negócio da FUNFER.

Para cumprimento dessa PSI, a FUNFER deve estabelecer estrutura de identificação de riscos e a criação de ambiente de controles internos que mitiguem a probabilidade de ocorrência de eventos que possam materializar tais riscos.

Deve-se criar um Plano de Continuidade de Negócios que aborde ações de gestão de riscos e de incidentes, incluindo os procedimentos que devem ser tomados em caso de vazamento e perda de informações, invasões de servidores, tempo de recuperação (RTO), ponto exato de recuperação das informações perdidas (RPO) e lista específica de quantas e quais autoridades relevantes devem ser acionadas para comunicação em tempo hábil em caso de ocorrência de um incidente (como vazamento de dados, por exemplo).

Caso ocorra algum incidente, o usuário da informação deve comunicar imediatamente o Departamento de TI para tratativas necessárias, e o departamento de TI deverá prontamente comunicar ao DPO, Jurídico e *Compliance* sobre o incidente fato, para avaliem eventuais riscos jurídicos e necessidade de tomada de medidas.

Rua Benedito Gonçalves, nº. 1801, Jardim Floramar, Divinópolis/MG
Funfer Fundição de Ferro
www.funfer.com.br
(37) 3512-4900

6. Controles de Acesso

O controle de acesso visa gerenciar e/ou restringir o acesso de pessoas aos ambientes físicos ou lógicos da FUNFER.

Para o cumprimento dessa PSI, é necessário o estabelecimento de diretrizes e responsabilidades de cada usuário em relação aos acessos à ambientes lógicos ou físicos da FUNFER, tais como:

- Diretrizes de segregação de função dos usuários;
- Definição de perfil com as devidas alçadas de aprovação por cargo e área;
- Critérios para autorização de acesso a espaços físicos;
- Restrição ao uso de hardwares externos não homologados pelo departamento de TI (ex. *pendrive* ou HD externos pessoais);
- Diretrizes para uso do *WhatsApp* como meio de comunicação.

Abaixo são descritos os ambientes de acesso divididos em 2 categorias: Lógico e Físico, e citada a necessidade de proteção para cada uma dessas categorias:

a. Acessos Lógicos

Criação do usuário

Toda pessoa que tenha o direito de acessar um ambiente lógico da FUNFER. Para cumprimento dessa PSI, o processo de criação de acesso deve seguir minimamente as seguintes diretrizes:

- Nome de usuário: cada usuário deve possuir um nome de identificação (login) de uso pessoal, individual e exclusivo;
- Perfil de acesso;
- Tempo de expiração do acesso (quando necessário);
- Medidas de segurança, por exemplo: direcionar que o usuário jamais compartilhe seus dados.

Senhas

A senha é recurso pessoal e intransferível utilizada no processo de verificação e autenticação da identidade de um usuário. Visa garantir que pessoas não autorizadas não possuam acesso às informações que são de responsabilidade de um determinado usuário, protegendo assim, sua integridade e segurança.

O processo de criação e atualização de senhas é de inteira responsabilidade do usuário, o qual deve envidar todos os esforços para mantê-la protegida.

A área de TI deve fornecer suporte necessário para que o usuário possa alterar sua senha em casos de primeiro acesso, criar e modificar sua senha tempestivamente.

Para o cumprimento dessa PSI é necessário que o procedimento em relação à criação de senhas de acesso contenha:

- Critérios de utilização de caracteres especiais e outras maneiras que fortaleçam a integridade na criação de senhas;
- Ambientes da FUNFER onde é necessário a criação e utilização de senhas, como por exemplo: Login em Notebooks, VPN, Redes de WI-FI, e demais locais definidos pela área de T.I.;
- Prazo de expiração da senha; (quando necessário)
- Critérios de cancelamento de senha.

Segurança nas Comunicações

As transmissões das informações devem ser protegidas com o objetivo de garantir sua segurança e integridade. Convém que as redes contenham controles implementados que assegurem que os serviços a ela conectados não sofram acessos desautorizados.

A segurança nas comunicações é baseada nas seguintes diretrizes:

- Definição de responsabilidades sobre o gerenciamento dos equipamentos de rede;
- Segregação de responsabilidades entre a área que gerencia as operações da rede e das demais áreas de TI;
- Implantação de controles que assegurem a confidencialidade e integridade dos dados;
- Implantação de mecanismos de registro, de monitoramento e de detecção de ações que possam expor a integridade das informações à riscos;
- Estabelecimento de restrição de acesso à rede;
- Segregação de redes: Dividir o armazenamento de informações em várias redes, como por exemplo, armazenar em uma rede os dados financeiros e em outra rede os dados de sistemas ou usuários;
- Homologação de ferramentas oficiais permitidas pela FUNFER para execução de tarefas diárias.
- Destruição de todos os arquivos físicos através de empresas especializada;

Dispositivos Móveis

Os dispositivos móveis são ativos da FUNFER e necessitam de cuidados pessoais em sua utilização, de maneira que não haja a exploração de vulnerabilidades por meio deles.

Para cumprimento desta PSI, deve-se elaborar um procedimento que permeie as diretrizes de mitigação de riscos inerentes ao uso de dispositivos móveis.

Deve-se considerar no documento de procedimento:

- O registro com os detalhes do aparelho e o seu responsável pela utilização;
- Critérios para instalação de aplicativos;
- Criação de senha de desbloqueio;
- Regras de utilização de redes sociais;
- Desativação e bloqueio do aparelho de forma remota.

☐ Uso de aplicativos como *WhatsApp:*

O uso de aplicativos de comunicação, como por exemplo, *WhatsApp,* devem preferencialmente, serem utilizados em dispositivos corporativos. Além disso, o uso do aplicativo deve seguir algumas diretrizes como:

a. Realizar a exclusão das informações e documentos recebidos/enviados pelo aplicativo mensalmente;
b. Utilizar a função "autenticação de dois fatores" do aplicativo, para assegurar maior segurança no tratamento de dados;
c. Reportar imediatamente à FUNFER perda do dispositivo móvel contendo o aplicativo.

Trabalho Remoto

O trabalho remoto é considerado como o exercício de atividades que são realizadas fora das dependências da FUNFER.

Para garantir que os usuários apliquem esforços para colaboração da segurança da informação, a FUNFER deve estabelecer diretrizes sobre os deveres para utilização de acesso remoto, as quais deve conter:

- Medidas adotadas para evitar a visualização das informações por pessoas não relacionadas às atividades, tais como amigos ou parentes quando os colaboradores estiverem em regime de trabalho híbrido ou em *home office*.
- Manuseio dos ativos, por exemplo: Evitar deixar o ativo (notebook, dispositivo móvel) em cima da mesa em momentos de refeição ou perto de locais com grande fluxo de pessoas.
- Bloqueio dos ativos: Sempre realizar o bloqueio da tela dos computadores;
- Políticas de segurança e privacidade dos ativos fornecidos;
- Em caso de trabalho remoto, utilizar apenas computadores e impressoras corporativos.

Perfis de acesso

Os perfis de acesso definem o nível de permissão que cada usuário possui para aprovações, exclusões e inserções manuais em um sistema de gestão.

Para cumprimento dessa PSI é necessária a definição de:

- Os tipos de perfis de acesso com suas respectivas nomenclaturas;
- O conteúdo de cada tipo de perfil de acesso;
- Área e cargo dos usuários e os respectivos perfis de acesso;
- Justificativa da alocação do perfil de acesso ao usuário;
- As segregações de funções, considerando alçadas de aprovação.

a. Acesso Físico

Acesso às áreas internas da FUNFER

O controle de acesso físico visa proteger o contato de pessoas não autorizadas com equipamentos, informações, áreas e usuários da FUNFER.

Para cumprimento dessa PSI é necessária a aplicação das seguintes diretrizes:

- Registro de acesso de toda e qualquer pessoa que acesse suas dependências físicas, incluindo visitantes, prestadores de serviço e/ou fornecedores, contendo os seguintes dados: nome do responsável pelo recebimento, área acessada, motivo do acesso e hora do acesso;
- Controle de acesso nas áreas internas, por exemplo: portas que necessitam do uso de crachás para acessar;
- Indicação de responsável para comunicação em caso de constatação de eventual invasão;

Rua Benedito Gonçalves, nº. 1801, Jardim Floramar, Divinópolis/MG
Funfer Fundição de Ferro
www.funfer.com.br
(37) 3512-4900

- Fechamento das portas dos ambientes que não estão em uso com a definição do responsável pelo trancamento;
- Estruturação de infraestrutura que evite que informações sejam ouvidas por pessoas não autorizadas em caso de reuniões ou ligações;
- As portas e as janelas possuam proteção e controle de acesso, fechaduras, trancas e chaves;
- Os corredores, portas e ambientes tenham uma sinalização específica, identificando-os de forma clara e precisa;
- Implantação de sistema de monitoramento e de detecção de intrusão.

7. Classificação da Informação

As informações possuem importância em diferentes níveis. Faz-se necessário que as informações sejam classificadas e que os controles e tratamentos realizados sejam estabelecidos.

Para o cumprimento dessa PSI é necessário o estabelecimento de uma Política de Classificação da Informação que contenha as diretrizes e responsabilidades de cada usuário em relação ao tema. O proprietário da informação deve ficar responsável por sua classificação.

A Política de Classificação de Informações deve conter:

- Controles de proteção associados às informações;
- Níveis da informação, por exemplo: Confidencial, Interna, Restrita ou Pública;
- Tempo de classificação;
- Grau de risco em caso de exposição;
- Responsável pelo acesso à informação.

8. Classificação de Dados Pessoais

A Política de Classificação de Dados deve estabelecer diretrizes sobre como deve ser realizada toda e qualquer classificação de dados pessoais que estejam em posse da FUNFER. Esta política visa a atender a Lei geral de Proteção de Dados ("LGPD") e deve conter as seguintes diretrizes:

- A classificação de informação é de competência do seu proprietário, qualificado em função do grau de confidencialidade exigido;

Rua Benedito Gonçalves, nº. 1801, Jardim Floramar, Divinópolis/MG
Funfer Fundição de Ferro
www.funfer.com.br
(37) 3512-4900

- Toda informação em meio físico ou digital deve ser definida como sigilosa (Interno) ou ostensiva (Pública) no ato de sua criação ou aquisição com um dos seguintes rótulos:
  a) Sigilosa: Confidencial, restrito ou Uso Interno;
  b) Ostensiva: Público.

- O rótulo de classificação:
  a) Mídia eletrônica transportável: obrigatório a inclusão do rótulo de classificação da informação na própria mídia;
  b) Documentos físicos e digitais: obrigatória a inclusão do rótulo de classificação da informação na capa do documento e rodapé de cada página.

- Informações relacionadas à FUNFER criadas/manuseadas, armazenadas, transportadas ou reproduzidas por terceiros devem seguir as mesmas regras de classificação apresentadas neste documento;
- Dados pessoais sensíveis devem ser tratados como CONFIDENCIAL, seguindo as diretrizes atuais da Lei Geral de Proteção de Dados (LGPD), de preferência anonimizados e/ou pseudonimizados;
- Anonimizar e a pseudonimizar os dados sempre que possível.

A Política de Classificação de Dados Pessoais é de responsabilidade de todos os colaboradores da FUNFER.

9. Ambiente de trabalho limpo

A Política do ambiente de trabalho limpo deve tratar sobre medidas que visam evitar a exposição de informações por parte da FUNFER.

A referida política deve possuir diretrizes sobre:

- A armazenagem de papéis ou mídias que contenham informações que possuam um responsável específico;
- Bloqueio da tela do computador quando não estiver em uso pelo usuário;
- Não deixar papéis e rastro de impressões nas impressoras.

Rua Benedito Gonçalves, nº. 1801, Jardim Floramar, Divinópolis/MG
Funfer Fundição de Ferro
www.funfer.com.br
(37) 3512-4900

- Cautela ao compartilhar telas em reuniões, sempre avisar quando iniciar a gravação.
- Cautela ao enviar e-mails internos ou externos, conferindo endereços adicionados.

10. Transferência de Informações

As transferências de informações podem ocorrer de várias formas dentro da FUNFER, as mais comuns são: e-mails, aplicativos de comunicação, via sistemas utilizados pela empresa e *WhatsApp*.

Para o cumprimento dessa PSI é necessário o estabelecimento de procedimento de transferência de informações que contenha as diretrizes e responsabilidades de cada usuário em relação ao tema.

O procedimento de transferência de informações deve conter as seguintes diretrizes:

- Senhas ou controle mitigatório que evite a ocorrência de cópias não autorizadas, modificação ou destruição das informações;
- A alocação das responsabilidades de cada usuário em caso de distorção das informações transmitidas;
- Uso de criptografia para assegurar a integridade e segurança da informação;
- Medidas de descarte e retenção de documentos físicos, como por exemplo: cartas, relatórios, notificações e afins;
- Restrições e orientações referentes ao encaminhamento de e-mails, e respostas automáticas;
- Medidas que assegurem que informações que contenham dados e/ou conteúdos sensíveis sempre sejam endereçadas e entregues aos correspondentes, nunca intermediando sua entrega;
- Controles para rastreabilidades das informações;
- Identificação dos emissores/portadores;
- Responsabilidade em caso de incidentes, como perda de dados;
- Evitar carregamento de celular, smartwatch ou outros dispositivos eletrônicos direto do notebook vinculado à FUNFER;
- Discussão de casos/processos em ambientes controlados.

11. Transferência Internacional de Dados

Para cumprimento dessa PSI é necessário que haja o estabelecimento de um procedimento que determine as diretrizes sobre as atividades que envolvem transferência internacional de dados, em

Rua Benedito Gonçalves, nº. 1801, Jardim Floramar, Divinópolis/MG
Funfer Fundição de Ferro
www.funfer.com.br
(37) 3512-4900

plena conformidade com a Política de Transferência Internacional de Dados. O objetivo deste procedimento é padronizar as atividades pertinentes à transferência de dados pessoais para um país estrangeiro, esse procedimento visa atender a LGPD.;

Abaixo constam algumas diretrizes contidas no procedimento de transferência de dados:

- O procedimento de transferência internacional de dados aplica-se às todas as transferências de dados pessoais efetuadas para países estrangeiros, sendo este documento aplicável à todas as empresas pertencentes à FUNFER e deve ser realizado em estrita conformidade com a Política de Transferência Internacional de Dados;
- A transferência de dados pessoais deverá ocorrer apenas se o país estrangeiro garantir um nível adequado de proteção aos dados igual ou superior ao requisitado pela LGPD, dessa forma, para localidades as quais não possuam legislações específicas de proteção de dados, a transferência ou o conjunto de transferências de dados pessoais devem ocorrer mediante a reserva de salvaguardas técnicas e jurídicas comprovadamente seguras e definidas em instrumentos próprios, de acordo com a LGPD
- Quaisquer incidentes de dados devem ser prontamente comunicados ao departamento de *Compliance,* Jurídico e DPO, bem como ao gestor da área;
- As transferências internacionais de dados devem ser permitidas apenas mediante a inserção de cláusula contratual padrão, adoção de mecanismos técnicos adequados, e reforçando o comprometimento do controlador/operador destinatário com as obrigações legais impostas pela LGPD, visando a preservação e segurança e confidencialidade das informações dos titulares de dados.

O Procedimento de transferência internacional de dados está em poder do DPO e *Compliance*, em conformidade com a Política de Transferência Internacional de Dados.

Observação: Ressalta-se que as transferências internacionais de dados podem ocorrer pelo simples fato de contratar serviços que utilizem servidores em outros países, portanto cada caso deve ser avaliado inicialmente pelo TI por meio da leitura e compreensão dos termos de uso de software de terceiros, bem como de eventuais contratos a serem assinados, relativos à parte técnica e armazenamento de dados.

12. Gerenciamento de Vulnerabilidades Técnicas

O gerenciamento de vulnerabilidades visa mitigar os riscos de incidentes por falhas técnicas.

Para o cumprimento dessa PSI é necessário o estabelecimento de um procedimento de gerenciamento de vulnerabilidade técnicas que contenha as diretrizes e responsabilidades de cada usuário em relação ao tema.

Os procedimentos devem conter diretrizes sobre:

- Inventário dos ativos que lidam com informações;
- Controle de instalação de softwares, contendo os dados do fornecedor, número da versão do software instalado, número do ativo;
- Especificar os responsáveis técnicos que devem ser procurados em caso de dúvidas e incidentes;
- Restrições à instalação de softwares;
- Indicação de responsáveis para avaliação em caso de necessidade de instalação de novos softwares;
- Requisitos para casos de auditoria (acesso apenas para leitura dos dados);
- Controle e gestão das informações com backups adequados.

13. Sanções e Punições

Se houver descumprimento das diretrizes dessa PSI, a FUNFER poderá aplicar sanções administrativas e/ou contratuais conforme os procedimentos disciplinares vigentes.

14. Revisões

Esta norma será revisada periodicamente de acordo com prazos estabelecidos pela área de T.I. ou mediante atualização extraordinária.

Data	Versão	Descrição	Autor	Aprovado por
25/08/2023	0.1	Criação	Departamento Jurídico e Compliance	Matheus Puppe