Política de Segurança da Informação		**Versão:** 01 **Data:** 27/04/2026
Áreas Envolvidas: HSC, Compliance, Jurídico.		
Público-alvo: Diretores, Colaboradores, Estagiários, Aprendizes, Prestadores de Serviço, Clientes, Fornecedores, Visitantes.		
Elaborada: Gerente de Tecnologia, DPO	**Revisada:** Comitê de Ética	**Aprovado:** Diretor Geral

1. Objetivo

A Política de Segurança da Informação (PSI) do Grupo Hardlink define as diretrizes essenciais para a proteção dos ativos de informação, assegurando a confidencialidade, integridade e disponibilidade dos dados.

Este documento constitui a base para o desenvolvimento de políticas complementares mais específicas, com o objetivo de manter um ambiente seguro e alinhado às melhores práticas de mercado e à legislação aplicável

Seu objetivo principal é estabelecer diretrizes e normas que garantam a proteção dos ativos de informação contra ameaças internas e externas, sejam elas intencionais ou acidentais. Além disso, busca assegurar a confidencialidade, integridade e disponibilidade das informações, incentivar o uso ético e responsável dos recursos tecnológicos e garantir a conformidade com requisitos legais e regulatórios, incluindo a Lei Geral de Proteção de Dados (LGPD).

2. Definições

Para os fins desta Política, 'Grupo Hardlink' refere-se à Hardlink e às demais empresas a ela vinculadas.

3. Abrangência

Esta Política se aplica a todos os indivíduos que, de alguma forma, têm acesso ou utilizam os ativos de informação do Grupo Hardlink. Isso inclui, mas não se limita ao público-alvo, independentemente de sua localização geográfica ou do tipo de dispositivo utilizado para acesso. A adesão a esta política é condição obrigatória para o acesso e uso dos recursos da empresa.

4. Riscos e Causas

O Grupo Hardlink reconhece que a segurança da informação está constantemente exposta a diversos riscos que podem comprometer seus ativos. As principais causas de incidentes de segurança incluem, mas não se limitam a:

- Divulgação não autorizada de informações sensíveis: Vazamento de dados confidenciais, seja por intenção maliciosa ou negligência.
- Perda ou roubo de dados: Ocorrência de extravio de dispositivos ou documentos contendo informações críticas.
- Acesso indevido: Utilização de credenciais ou privilégios de acesso de forma não autorizada.
- Alteração ou destruição de dados: Modificação ou exclusão de informações sem permissão, comprometendo sua integridade.
- Indisponibilidade de sistemas: Falhas técnicas, ataques cibernéticos ou desastres que impeçam o acesso às informações e serviços.
- Ataques de malware e phishing: Infecções por softwares maliciosos ou tentativas de engenharia social para obtenção de informações.

- Negligência ou desconhecimento: Falta de atenção ou treinamento adequado por parte dos usuários, resultando em vulnerabilidades.
- Violações de conformidade: Descumprimento de leis, regulamentos ou políticas internas, gerando riscos legais e reputacionais.

5. Referências Normativas

Esta Política é fundamentada e complementada pelas seguintes referências normativas e legais:

- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD): Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
- Normas ISO/IEC 27001 e 27002: Padrões internacionais para sistemas de gestão de segurança da informação e códigos de prática para controles de segurança da informação, respectivamente.
- Normas ABNT: Normas técnicas brasileiras aplicáveis à gestão da segurança da informação.
- Código de Ética e Conduta do Grupo Hardlink: Documento interno que estabelece os princípios morais e éticos que devem guiar o comportamento de todos os colaboradores, estagiários, aprendizes, prestadores de serviços, fornecedores, clientes e parceiros.

6. Conceitos

Para os fins desta Política, os termos abaixo possuem os seguintes significados:

- **Informação:** Dados, fatos, conhecimentos ou quaisquer outros conteúdos, em qualquer formato (digital, físico, verbal), que possuam valor para o Grupo Hardlink;
- **Ativo de Informação:** Qualquer item que possua valor para o Grupo Hardlink e que esteja relacionado à informação, incluindo hardware, software, dados, documentos, serviços e pessoas;
- **Equipamento:** Qualquer dispositivo eletrônico ou físico fornecido pelo Grupo Hardlink ou de propriedade do usuário, utilizado para acessar ou processar informações da empresa (ex: notebooks, desktops, smartphones, tablets);
- **Aplicativo**: Qualquer programa de computador, sistema ou serviço online utilizado para fins de trabalho ou que processe informações do Grupo Hardlink;
- **Recurso de TI:** Qualquer componente de tecnologia da informação, incluindo redes, servidores, sistemas operacionais, bancos de dados e serviços de nuvem.
- **Colaborador (Empregado):** Qualquer pessoa física com vínculo empregatício direto com o Grupo Hardlink.
- **Prestador de Serviços:** Pessoa física ou jurídica que presta serviços ao Grupo Hardlink, tendo acesso, direto ou indireto, aos seus ativos de informação.
- **Ambiente:** Qualquer local físico ou lógico onde os ativos de informação do Grupo Hardlink são armazenados, processados ou transmitidos.
- **Identidade Lógica:** Conjunto de credenciais (usuário e senha, certificado digital, etc.) que permite a um indivíduo autenticar-se e acessar os recursos de TI do Grupo Hardlink.
- **Confidencialidade:** Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.
- **Integridade:** Propriedade de salvaguardar a exatidão e a completude da informação e dos métodos de processamento.
- **Disponibilidade:** Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.

7. Regras Gerais

As seguintes regras gerais são mandatórias para todos os abrangidos por esta Política, visando a proteção dos ativos de informação do Grupo Hardlink:

7.1. Código de Ética e Conduta e Termo de Confidencialidade e Conduta

Todos os colaboradores, estagiários, aprendizes, prestadores de serviços, fornecedores, clientes, parceiros devem aderir integralmente ao **Código de Ética e Conduta** e assinar um **Termo de Confidencialidade e Comprometimento** no momento de sua admissão ou contratação. Estes documentos reforçam as obrigações de sigilo e o uso adequado das informações e recursos da empresa.

7.2. Comitê de Segurança da Informação (CSI)

Será instituído um **Comitê de Segurança da Informação (CSI)**, composto por representantes da área de TI, do Encarregado de Dados (DPO), do Departamento de Recursos Humanos e um representante da alta direção.

O CSI será responsável por:

- Revisar e aprovar as políticas de segurança da informação.
- Analisar e deliberar sobre incidentes de segurança de alta gravidade.
- Definir e aprovar perfis de acesso a sistemas e equipamentos [ref. PSI.06.02.01].
- Acompanhar a implementação das ações de segurança.
- Atuar como instância decisória para casos omissos ou de difícil resolução.

7.3. Gestão de Riscos em Projetos

Todos os novos projetos e iniciativas que envolvam o tratamento de informações ou o uso de novos recursos de TI devem incluir uma etapa de **Análise e Mapeamento de Riscos de Segurança da Informação**. Esta análise deve ser conduzida pela equipe de TI em conjunto com o CSI, garantindo que as medidas de segurança sejam incorporadas desde a concepção do projeto.

7.4. Responsabilidades Gerais

A segurança da informação é uma responsabilidade compartilhada. As responsabilidades específicas são detalhadas em políticas complementares, mas as diretrizes gerais são:

- Todos os Colaboradores, estagiários, aprendizes, Prestadores de Serviços, fornecedores, clientes, parceiros: Cumprir integralmente esta Política e suas políticas complementares;
- Proteger as informações e os ativos do Grupo Hardlink sob sua responsabilidade;
- Reportar imediatamente qualquer incidente ou suspeita de violação de segurança ao Service Desk ou ao CSI;
- Utilizar os equipamentos e aplicativos do Grupo Hardlink de forma ética e responsável, conforme a Política de Responsabilidade e Uso de Equipamentos e Aplicativos;
- Diretores e Gerentes: Garantir que suas equipes compreendam e cumpram as políticas de segurança da informação.
- Promover a cultura de segurança da informação em suas respectivas áreas.
- Alocar recursos necessários para a implementação das medidas de segurança.
- Equipe de Tecnologia da Informação (TI): Implementar, manter e monitorar os controles de segurança tecnológica.
- Gerenciar acessos a sistemas e redes, conforme a Política de Monitoramento, Acesso e Identidade;
- Responder a incidentes de segurança e realizar análises forenses, conforme a Política de Tratamento de Incidentes e Violações;
- Fornecer treinamento e conscientização em segurança da informação;

- Encarregado de Dados (DPO): Atuar como canal de comunicação entre o Grupo Hardlink, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- Orientar sobre as melhores práticas de proteção de dados pessoais;
- Garantir a conformidade com a LGPD.

7.5 Disposições Gerais

Esta Política entra em vigor na data de sua divulgação, por prazo indeterminado, devendo ser revisada, no mínimo, a cada 24 meses.

Para detalhes específicos sobre uso de equipamentos, monitoramento, classificação de dados, tratamento de incidentes e responsabilidades de prestadores, consulte os módulos complementares:

- Política de Responsabilidade e Uso de Equipamentos e Aplicativos;
- Política de Monitoramento, Acesso e Identidade;
- Política de Classificação e Proteção da Informação;
- Política de Tratamento de Incidentes e Violações.

7.6 Histórico de Revisões

Data da Revisão	Versão	Motivo
28/08/2022	00	Criação
27/04/2026	01	Revisão Geral