HIGHPAR

Política de Segurança Cibernética

Versão	Revisado em:	Aprovado Por:
1.1	novembro de 2025	Comitê de Compliance e PLDFT

HIGHPAR

Sumário

1. Introdução e Objetivo

O grupo Highpar

O Grupo Highpar é um grupo econômico independente do mercado financeiro brasileiro, que atua de forma integrada nas áreas de gestão de recursos, investimentos e consultoria financeira, comprometido com os mais elevados padrões de governança, transparência e conformidade regulatória.

O Grupo é formado por empresas especializadas que atuam de maneira complementar, e conta com as empresas: **High Asset Management LTDA** (gestora de valores mobiliários), **High Gestão e Investimentos LTDA** (gestora de valores mobiliários), **High Wealth Management LTDA** (gestora de valores mobiliários), **High Investment Advisory LTDA** (consultora de valores mobiliários), **High Capital Markets** (consultoria imobiliária), **High Desenvolvimento Imobiliário LTDA** (gestão imobiliária) e **High Realty Participações LTDA** (investimentos imobiliários).

A atuação conjunta dessas entidades reflete o compromisso do Grupo Highpar com a solidez operacional, a governança corporativa, gestão de conflitos de interesse e a geração de valor sustentável, integrando processos de compliance, gestão de risco, controles internos e prevenção à lavagem de dinheiro (PLD/FTP) em todas as suas frentes de negócio.

1.1. Propósito do Manual

Este Manual estabelece as diretrizes, princípios e procedimentos para a proteção dos ativos de informação da Highpar contra ameaças cibernéticas. A segurança cibernética é um pilar estratégico para a continuidade dos negócios, proteção de dados de clientes e conformidade regulatória.

O objetivo é criar uma cultura de segurança robusta, detalhando responsabilidades, gestão de riscos, controles e planos de resposta a incidentes para garantir a confidencialidade, integridade e disponibilidade das informações.

1.2. Abrangência e Base Legal

Esta política aplica-se a todas as áreas, processos, sistemas, informações, colaboradores da Highpar e terceiros que acessam dados da instituição, incluindo

dispositivos corporativos ou pessoais (quando em uso para trabalho) e serviços em nuvem.

A elaboração segue as diretrizes da CVM (Resolução CVM nº 35), ANBIMA (Guia de Cibersegurança, Regras e Procedimentos de Deveres Básicos, Orientações para Contratação de Terceiros e Nuvem) e melhores práticas internacionais (NIST).

1.3. Princípios Fundamentais de Segurança Cibernética

- **Confidencialidade:** Garantir que informações sejam acessíveis apenas por pessoas autorizadas.
- **Integridade:** Assegurar que as informações sejam precisas, completas e não tenham sido alteradas de forma não autorizada.
- **Disponibilidade:** Garantir que sistemas e informações estejam acessíveis quando necessário.
- **Resiliência:** Capacidade de resistir, adaptar-se e recuperar-se rapidamente de interrupções, como ataques cibernéticos.
- **Prevenção:** Implementar medidas proativas para evitar incidentes.
- **Detecção:** Identificar rapidamente a ocorrência de um incidente.
- **Resposta:** Reagir de forma eficaz para minimizar impactos.
- **Recuperação:** Restabelecer sistemas e dados afetados.
- **Conformidade:** Assegurar a aderência a leis, regulamentações e políticas internas.
- **Conscientização:** Promover educação e treinamento contínuo dos colaboradores.

2. Governança e Estrutura Organizacional

A governança de segurança cibernética estabelece responsabilidades claras e alinha as decisões de segurança aos objetivos de negócio.

2.1. Papéis e Responsabilidades

- **Diretoria de Risco e Compliance:** Responsável pela aprovação da Política, alocação de recursos e supervisão geral da gestão de riscos cibernéticos, integrando-a à estratégia de negócios.
- **Diretor de Risco e Compliance:** É o diretor estatutário responsável pela supervisão do programa de segurança cibernética. Atua como ponto focal e deve:
    - Coordenar a implementação e revisão da Política.
    - Supervisionar a gestão de riscos cibernéticos (identificação, avaliação e tratamento).
    - Garantir a conformidade regulatória.
    - Reportar à alta direção sobre o status da segurança cibernética.
    - Promover a conscientização e o treinamento.
- **Área de Tecnologia da Informação (TI):** Responsável pela implementação e manutenção dos controles técnicos de segurança e pela resposta inicial a incidentes.
- **Diretoria de Compliance:** Garante que as políticas estejam em conformidade com as leis (LGPD, CVM, ANBIMA).
- **Todos os Colaboradores e Terceirizados:** Devem seguir as políticas, proteger as informações e reportar atividades suspeitas ou incidentes.

2.2. Comitê de Risco e Compliance

Este comitê é composto por representantes da alta direção, Diretor de Compliance, responsável pelo TI, jurídico e outras áreas relevantes. Suas funções incluem:

- Propor e revisar a estratégia de segurança cibernética.
- Analisar e aprovar políticas e procedimentos.
- Monitorar o cenário de ameaças e a eficácia dos controles.
- Supervisionar a gestão de incidentes relevantes.
- Recomendar a alocação de recursos.
- Assegurar a comunicação eficaz sobre o tema.

3. Gestão de Riscos Cibernéticos

A gestão de riscos é um processo contínuo para identificar, avaliar, tratar e monitorar ameaças e vulnerabilidades.

3.1. Identificação e Avaliação de Riscos (Risk Assessment)

A Highpar realiza uma avaliação de riscos sistemática e periódica, que inclui:

- **Identificação de Ativos:** Mapeamento de hardware, software, dados, processos e serviços (internos ou terceirizados, incluindo nuvem).
- **Classificação da Informação:** Estabelecimento de regras para manuseio, armazenamento, transporte e descarte, considerando confidencialidade, integridade e disponibilidade.
- **Análise de Impacto:** Avaliação dos impactos (financeiro, operacional, regulatório, reputacional) e da probabilidade de ocorrência de eventos.
- **Revisão Periódica:** A avaliação é revisada anualmente ou sempre que houver mudanças significativas no ambiente.

3.2. Ações de Prevenção e Proteção

- **Controle de Acesso:** Implementação de controles rigorosos (identificação, autenticação com múltiplos fatores sempre que possível, autorização). O acesso segue o princípio do menor privilégio e é revogado quando não mais necessário.
- **Gestão de Senhas:** Exigência de senhas complexas, proibição de reaproveitamento e recomendação de uso de gerenciadores.
- **Configuração Segura (*Hardening*):** Equipamentos e sistemas devem ser configurados de forma segura e testados em homologação antes da produção.
- **Proteção contra Malware:** Implementação de soluções antivírus, anti-malware e IDS/IPS.

- **Criptografia:** Utilização para proteger dados sensíveis em repouso e em trânsito.
- **Segurança de Redes:** Implementação de firewalls e segmentação de redes.
- **Backup e Recuperação:** Realização de backups regulares e testados, com cópias armazenadas de forma segura e criptografada.

4. Proteção de Dados e Privacidade – LGPD

A Highpar está comprometida em proteger informações pessoais e sensíveis, em conformidade com a Lei Geral de Proteção de Dados (LGPD).

4.1. Classificação da Informação

A instituição adota um processo de classificação da informação (ex: público, interno, confidencial, restrito) para identificar dados com base em sua sensibilidade e criticidade, orientando a aplicação de controles adequados.

4.2. Controles de Acesso

Os controles de acesso são baseados no princípio do menor privilégio e na necessidade de conhecimento.

- **Gestão de Identidade e Acesso:** Gerenciamento do ciclo de vida das identidades digitais (criação, alteração, desativação).
- **Segregação de Funções:** Implementada para evitar que um único indivíduo controle etapas de um processo crítico.
- **Monitoramento de Acessos:** Registro e auditoria de acessos para identificar atividades suspeitas.

4.3. Conformidade com a LGPD

A Highpar está em conformidade com a Lei nº 13.709/2018. As ações incluem:

- Atendimento aos princípios da LGPD (finalidade, necessidade, transparência, segurança, etc.).
- Disponibilização de uma Política de Privacidade clara.

- Implementação de mecanismos e boas práticas de Segurança da Informação para mitigar riscos de acesso indevido ou vazamento de dados pessoais.
- Regras para gerenciamento de identidade e acesso aos dados pessoais.

5. Segurança da Informação e Controles Técnicos

Medidas técnicas são implementadas para proteger a infraestrutura e os dados.

- **Segurança de Redes:**
  - **Firewalls:** Utilizados para controlar o tráfego de rede (entrada e saída) e bloquear acessos não permitidos.
  - **IDS/IPS:** Sistemas de Detecção e Prevenção de Intrusões monitoram o tráfego em busca de atividades maliciosas, podendo bloquear tráfego suspeito.
- **Segurança de Endpoints:**
  - **Antivírus e Anti-Malware:** Soluções instaladas e atualizadas em todos os endpoints.
  - **Controle de Dispositivos Removíveis:** Políticas para controlar o uso de USB e outras mídias.
  - **Configuração Segura *(Hardening)*:** Aplicação de configurações rigorosas, desativando serviços desnecessários.
- **Gestão de Vulnerabilidades:**
  - Processo proativo para identificar e remediar falhas de segurança.
  - **Varreduras de Vulnerabilidade:** Realização periódica de varreduras automatizadas.
  - **Monitoramento de Ameaças:** Acompanhamento de feeds de inteligência.

6. Gestão de Incidentes Cibernéticos

Processo visa minimizar o impacto de eventos adversos e garantir a rápida recuperação.

6.1. Detecção e Análise de Incidentes

- **Alertas e Notificações:** Configuração de alertas automáticos para eventos críticos.
- **Análise Forense:** Capacidade de determinar a causa raiz e o escopo do incidente.
- **Inteligência de Ameaças:** Utilização para identificar Indicadores de Comprometimento.

6.2. Contenção, Erradicação e Recuperação

- **Contenção:** Medidas para isolar os sistemas afetados e impedir a propagação do incidente.
- **Erradicação:** Remoção da causa raiz do incidente (ex: malware, vulnerabilidades).
- **Recuperação:** Restauração dos sistemas e dados a um estado operacional seguro, utilizando backups e validando a integridade.

7. Treinamento e Conscientização

O fator humano é crítico, exigindo investimento contínuo em treinamento para promover uma cultura de segurança.

7.1. Programa de Treinamento e Conscientização

A Highpar trata da segurança cibernética em seu treinamento de procedimentos internos, estabelecendo um programa estruturado para todos os colaboradores, com os objetivos de:

- Desenvolver competências para identificar e reportar ameaças.
- Disseminar conhecimento sobre políticas, regras e boas práticas.
- Disponibilizar materiais sobre ameaças (phishing, ransomware, engenharia social).

- Estimular o engajamento e a adoção de comportamentos seguros.
- Avaliar a eficácia dos treinamentos na redução de riscos.

7.2. Conteúdo e Metodologia

O conteúdo é adaptado a cada público.

- **Conteúdo:** Boas práticas (uso seguro de e-mail, senhas, internet), tipos de ameaças e políticas internas.
- **Metodologia:** Treinamento obrigatório anual, testes, campanhas e reciclagens.

7.3. Avaliação e Melhoria Contínua

A eficácia do programa é avaliada continuamente, incluindo:

- Monitoramento da participação e aprendizado.
- Exercícios de verificação sobre conceitos e ameaças.
- Análise do impacto na redução de incidentes.
- Revisão e aprimoramento do programa com base nos resultados e no cenário de ameaças.

8. Revisão e Atualização da Política

A Política será revisada e atualizada no mínimo anualmente, ou sempre que ocorrerem mudanças significativas (regulatórias, tecnológicas, organizacionais). A aprovação das atualizações compete ao Comitê de Risco e Compliance e à Diretoria Executiva.