Diretrizes da Política de Segurança Cibernética

HS financeira

Uma empresa do Grupo Herval

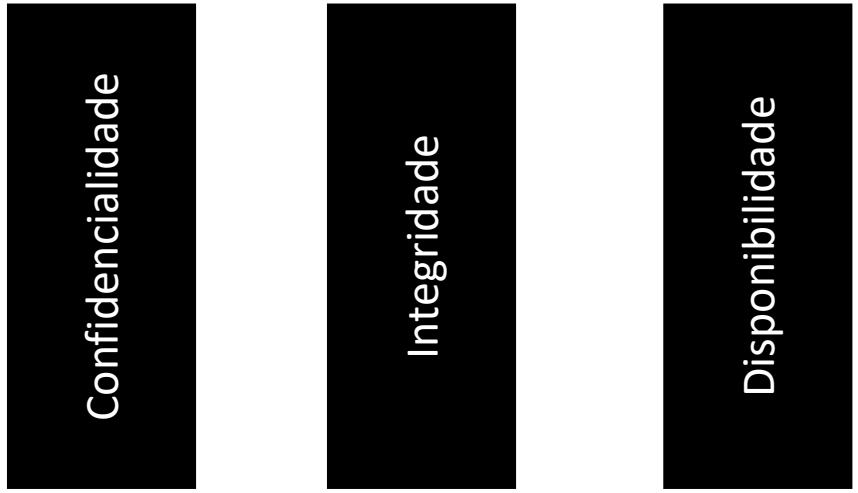
Objetivo

O objetivo do documento Diretrizes da Política de Segurança Cibernética é definir as condutas que a Instituição deve adotar para a proteção e o tratamento dos riscos relacionados aos seus ativos estratégicos.

Os princípios aqui estabelecidos devem ser observados por todos, colaboradores, prestadores de serviço e correspondentes no país, na execução de suas funções, utilizando-se dos meios físicos ou lógicos da Instituição.

Pilares da Segurança Cibernética

A área de Segurança da Informação é responsável por estabelecer padrões, procedimentos e controles que garantam a segurança das informações presentes nos processos e rotinas da Instituição. A área busca minimizar possíveis impactos e riscos de incidentes de segurança que afetem os negócios da organização. Frente a essas responsabilidades, a conduta da Instituição é guiada por três pilares essenciais de segurança:



Pilares da Segurança Cibernética

- ✓ **Confidencialidade:** garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas autorizadas;
- ✓ **Integridade:** garantir que as informações sejam mantidas íntegras, sem modificações indevidas, seja de forma acidental ou proposital;
- ✓ **Disponibilidade:** garantir que as informações estejam disponíveis e não afetem o andamento das rotinas da Instituição.

Responsabilidade da Segurança Cibernética

A Segurança Cibernética tem como objetivo e responsabilidade identificar, proteger, detectar, responder e recuperar a Instituição frente a uma possível ameaça, garantindo a confidencialidade, integridade e disponibilidade dos ativos estratégicos. Neste contexto, utilizam-se os conceitos:

- ❑ **Ataque Cibernético:** A exploração por parte de um agente malicioso tirando proveito de uma vulnerabilidade com a intenção de causar um impacto negativo a um alvo;
- ❑ **Ativos Estratégicos:** Todo e qualquer dispositivo físico ou digital, equipamento, dado, informação, ou outro componente que suporte os processos e rotinas da organização;
- ❑ **Incidente Cibernético:** Todo e qualquer evento inesperado que gere algum tipo de instabilidade, quebra de política ou que possa causar danos à organização.

Diretrizes gerais

i. Para que sejam adequadamente protegidas e não ocorram erros durante o seu tratamento, as informações são classificadas da seguinte forma:

- ✓ **Pública:** Informação/dado que pode ser divulgado ao público geral sem causar danos à organização, sendo considerado de baixa relevância;

- ✓ **Interna:** Informação/dado que pode ser divulgado entre os colaboradores da organização durante a execução de suas funções. Sua divulgação ou acesso indevido pode causar danos à organização, sendo considerado de média relevância;

- ✓ **Confidencial:** Informação/dado interno cuja divulgação pode causar danos financeiros e/ou à imagem da organização, podendo gerar vantagens à concorrentes e perda de clientes.

As informações ou dados, seja no período de geração, armazenamento, uso, transferência e destruição, devem ser tratados em conformidade com a sua classificação.

Toda a informação/dado deverá ser classificado quando for criado/armazenado. Todos – colaboradores, prestadores de serviços, terceirizados ou estagiários – deverão respeitar o nível de segurança da informação de acordo com a sua classificação ao realizarem as suas funções diárias.

Informação/dado:	**Grau de relevância:**
Público	Baixo
Interno	Médio
Confidencial	Alto

Diretrizes gerais

ii. Manter a capacidade de prevenir, detectar e reduzir a vulnerabilidade à incidentes relacionados com o ambiente cibernético, utilizando-se de registros de rastreabilidade dos dados;

iii. Assegurar que os dados da Instituição e de seus clientes sejam acessados e manipulados apenas por pessoas autorizadas, de forma segura e em conformidade com os princípios da Lei Geral de Proteção de Dados;

iv. Proteger ativos tecnológicos e estabelecer procedimentos de monitoramento das redes da companhia e das máquinas de funcionários para detecção de intrusões;

v. Conduzir monitoramento e resposta de incidentes, seguindo as etapas do Plano de Ação e Resposta a Incidentes e do Plano de Continuidade de Negócios;

vi. Garantir a conscientização da equipe através da disseminação da cultura de segurança da informação e cibernética.

Vigência

A Política de Segurança Cibernética da HS Financeira é vigente no âmbito da Instituição, dos correspondentes no país por ela contratados e pelos prestadores de serviços com os quais mantém relacionamento, sendo revisada, no mínimo, anualmente.

HS financeira

Uma empresa do Grupo Herval