

# Banco Hyundai Capital Brasil

## Política de Segurança da Informação

### 1. SEGURANÇA DA INFORMAÇÃO

Conheça os processos e controles que o **Banco Hyundai Capital Brasil S/A (BHCB)** estabelece para proteção da informação e tratamento dos riscos e ameaças relacionadas à Segurança da Informação.

Os princípios de Segurança da Informação estabelecidos neste documento possuem total aderência da alta administração da organização. São observados por todos na execução de suas funções, incluindo as instituições financeiras e demais sociedades autorizadas a funcionar pelo Banco Central do Brasil integrantes do Conglomerado Econômico-Financeiro do Banco Hyundai que a ela tenham expressamente aderido.

### 2. RESPONSABILIDADES E OBJETIVOS DA SEGURANÇA DA INFORMAÇÃO

A área de Segurança da Informação do Banco Hyundai é responsável por estabelecer, por meio da definição de políticas, padrões, procedimentos e controles, a integridade, disponibilidade e confidencialidade das informações contidas nos ambientes da organização. O objetivo é minimizar possíveis impactos e vulnerabilidades e reduzir a ocorrência de incidentes de segurança que afetem os negócios do Banco Hyundai. A disciplina concentra esforços contínuos para proteção dos ativos de informação, auxiliando a organização a cumprir sua missão e valores. Conheça nossos objetivos:

- **Confidencialidade:** visa garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas.
- **Integridade:** busca garantir que as informações sejam mantidas íntegras, sem modificações indevidas (acidentais ou propositas).
- **Disponibilidade:** garante que as informações estejam disponíveis às pessoas autorizadas

### **3. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO DO BANCO HYUNDAI**

#### **3.1. Proteção da Informação**

É diretriz que toda informação de propriedade do Banco Hyundai seja protegida de forma a não comprometer a sua confidencialidade, integridade ou disponibilidade, independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada.

#### **3.2. Gestão, controle de acessos e rastreabilidade**

Os acessos às informações são realizados somente mediante autorização do responsável pela informação e são restritos a pessoas autorizadas.

#### **3.3. Autenticação**

Todo empregado, estagiário ou prestador de serviços possui apenas um identificador (login) de acesso à informação.

#### **3.4. Prevenção contra vírus, arquivos e softwares maliciosos**

A organização tem controles para prevenir que vírus e outros tipos de softwares maliciosos entrem e se espalhem nos sistemas de informação por meio de arquivos e softwares não homologados cuja instalação e uso são proibidos.

#### **3.5. Manutenção e cópias de segurança**

A organização conta com procedimentos específicos para garantir a recuperação de dados e informações quando necessário.

#### **3.6. Classificação dos dados e das informações**

A organização adota quatro categorias para efeitos de classificação da informação:

- Público;
- Interno;
- Confidencial; ou
- Reservado.

### **3.7. Conscientização em Segurança da Informação**

O Banco Hyundai pratica a disseminação da cultura de Segurança da Informação aos seus empregados, prestadores de serviços e estagiários por meio de treinamentos específicos focados em garantir a confidencialidade, integridade e disponibilidade das informações.

### **3.8. Mesa limpa e descarte de informações**

O Banco Hyundai tem práticas orientadas aos empregados, prestadores de serviço e estagiários para que não deixem informações à mostra e as descartem sempre que necessário.

### **3.9. Confidencialidade**

Os contratos firmados com o Banco Hyundai possuem cláusula de confidencialidade.

### **3.10. Utilização dos recursos da informação**

O Banco Hyundai possui práticas em que apenas softwares disponibilizados e equipamentos configurados de acordo com o padrão da organização podem ser usados pelos empregados, prestadores de serviço e estagiários.

### **3.11. Prevenção a vazamento de informações**

O Banco Hyundai tem controles e políticas que previnem o vazamento de informações estabelecendo boas práticas para uso de correio eletrônico, acesso à internet, acesso remoto, uso de telefones móveis, comportamento dos empregados, prestadores de serviços e estagiários em locais públicos e na troca de informações com fornecedores.

## **4. ADERÊNCIA À POLÍTICA**

Caso seja identificada uma conduta não aderente à referida política, ou o seu descumprimento, o Banco Hyundai tomará as medidas legais, tecnológicas ou disciplinares necessárias de forma a manter a aderência à política.

\*\*\*\*\*