Banco Hyundai Capital Brasil

Política de Segurança Cibernética

1) SEGURANÇA CIBERNÉTICA

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

Os princípios de Segurança Cibernética 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 CIBERNÉTICA

A área de Segurança Cibernética do Banco Hyundai é responsável por identificar, proteger, detectar, responder e recuperar rapidamente de uma ameaça cibernética, a fim de proteger a confidencialidade, integridade e disponibilidade dos ativos tecnológicos e informações. Buscamos identificar:

- Incidentes cibernéticos: todo e qualquer evento não esperado que gere algum tipo de instabilidade, quebra de política ou que possa causar danos ao Banco Hyundai.
- Ataque cibernético: é a exploração por parte de um agente malicioso para tirar proveito de ponto(s) fraco(s) com a intenção de alcançar um impacto negativo no alvo. Os atacantes podem ter como alvo os clientes, fornecedores e parceiros do Banco Hyundai para causar impacto significante para a organização.
- Ativos tecnológicos: é qualquer dispositivo físico ou digital, equipamento ou outro componente do ambiente que suporte atividades relacionadas à informação.

3) RESPOSTA, TRATAMENTO DE INCIDENTES DE SEGURANÇA CIBERNÉTICA E CONTINUIDADE DE NEGÓCIOS

3.1. Tratamento de incidentes cibernéticos

O Banco Hyundai conta com mecanismos para prevenção de ameaças de origem cibernética. Todo e qualquer incidente de segurança cibernética, passa por uma análise e é classificado de acordo com o impacto causado pelo incidente, que pode ser crítico ou baixo de acordo com a classificação vigente. Caso um incidente de origem cibernética seja identificado pelo público geral ele deverá ser reportado pelo e-mail hcsirt@br.hcs.com.

3.2. Gestão de continuidade de negócios

A GCN (Gestão de Continuidade de Negócios) tem por objetivo avaliar a necessidade do desenvolvimento e implantação do PCN (Plano de Continuidade de Negócios), identificando procedimentos e infraestrutura alternativa para proteger as pessoas, a reputação, os valores e os compromissos com os públicos relacionados.

Para administrar crises, há uma governança pré-estabelecida, com membros previamente definidos. A responsabilidade é de administrar situações especiais, caso ocorra uma situação de excepcionalidade, diferente da esperada ou que deva derivar da gestão ordinária dos negócios. O objetivo é identificar o que possa comprometer o desenvolvimento das atividades ou acarretar em uma deterioração grave na situação financeira da entidade ou do grupo, por conjeturar um afastamento significativo do apetite ao risco e dos limites definidos.

O Banco Hyundai possui mecanismos de acionamento dos planos de continuidade de negócios em caso de desastres, tanto de origem cibernética como operacional.

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.

*****