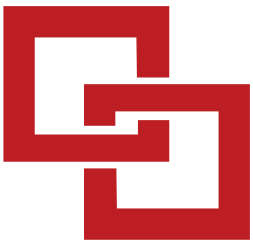

BRCARD

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Sumário:

1. OBJETIVO

A BRCARD estabelece a presente Política de Segurança Cibernética, alinhada as orientações do CMN através da resolução nº 4.658 de 26 de Abril de 2018, com o objetivo de aplicar os princípios e diretrizes de proteção das informações consideradas sensíveis da instituição e de seus clientes.

O Conselho de Administração e a Diretoria Executiva comprometem-se, por meio dessa Política, a oferecer os recursos necessários à melhoria contínua dos procedimentos relacionados à segurança cibernética, mantendo, com o menor risco possível, um ambiente computacional seguro.

2. PÚBLICO-ALVO

Esta Política tem caráter público e terá sua divulgação realizada por meio do sítio da BRCARD na Internet.

3. RESPONSABILIDADES

A Referida Política, foi aprovada pela Diretoria da BRCARD, implementada por sua Diretoria Administrativa, sendo de responsabilidade de todos os colaboradores e prestadores de serviços, com a abrangência sobre as atividades que envolvam dados e informações no ambiente cibernético.

Quaisquer indícios de incidentes ou irregularidades citadas nesta Política, devem ser comunicadas ao departamento de Compliance e ouvidoria da BRCARD pelo e-mail: ouvidoria@brcardcrediario.com

4. ESCOPO E DIRETRIZES GERAIS:

I- A Política é orientada como parte essencial e integrada aos processos e negócios da BRCARD.

II- Como forma de reduzir as vulnerabilidades dos ativos de informação, a BRCARD adota procedimentos e os controles baseados em autenticação, criptografia, prevenção e detecção de intrusão, prevenção de vazamento de informações, proteção contra software malicioso, mecanismos de rastreabilidade, controles de acesso e segmentação de rede de computadores e manutenção de cópias de segurança dos dados e das informações;

III- Prestadores de serviço, fornecedores e empresas conveniadas devem adotar procedimentos e controles compatíveis com os riscos envolvidos na prestação de serviços relevantes prestados junto aos clientes, para a preservação e continuidade das operações da BRCARD.

IV- As informações são devidamente classificadas de acordo com a confidencialidade e as proteções necessárias, devem ser tratadas de forma ética e sigilosa e de acordo com a regulamentação vigente.

V- O acesso às informações só deve ser feito se devidamente autorizado, e o acesso deverá ser realizado por meio de credencial única, pessoal, intransferível e identificável.

VI- A BRCARD possui Plano de Continuidade de TI (PCTI), que abrange as estratégias necessárias à continuidade dos serviços de TI essenciais: contingência, continuidade e recuperação e está voltado a garantir a continuidade aos processos definidos como críticos para a TI da BRCARD e serviços essenciais para seus clientes.

VII- Quaisquer riscos às informações dos clientes da BRCARD devem ser comunicados diretamente à Diretoria ou por meio dos canais de ouvidoria oferecidos pela BRCARD aos seus clientes.

VIII- A BRCARD atuará na disseminação da cultura de segurança cibernética, incluindo a conscientização dos seus clientes e usuários de produtos e serviços.

IX- A efetividade da Política Corporativa de Segurança Cibernética é verificada por meio de avaliações independentes periódicas de auditoria interna e externa, incluindo órgãos de controle e reguladores.

5. BASE NORMATIVA

. Resolução CMN nº 4.893, de 26 de fevereiro de 2021
. Resolução CMN nº 4.658 de 26 de Abril de 2018
. Lei Geral de Proteção de Dados : lei nº 13.709, de 14 de agosto de 2018

Criação /revisão: Thales Valadão/Dalton Tanure/ Oinnos Consultoria Tecnológica.
Versão: 01/2020
Aprovação: Juarez Faria/Thales Valadão/ Marco Perroni
Data: 28/10/2020