POLÍTICA DE CIBERSEGURANÇA

BANCO BNP PARIBAS BRASIL S.A – PRODUTO CETELEM

Fevereiro/2019

ÍNDICE

OBJETIVO **3**

DISPOSIÇÕES GERAIS **3**

- **Abrangência** **3**
- **Diretrizes** **3**
- **Aspectos gerais** **3**
- **Identificação** **3**
- **Proteção** **3**
- **Detecção** **4**

RESPONSABILIDADES **4**

MEDIDAS DISCIPLINARES **4**

REFERÊNCIAS **4**

GLOSSÁRIO **5**

OBJETIVO

Em linhas gerais, essa política tem como objetivo:

- Estabelecer as diretrizes de cibersegurança, visando proteger os ativos de tecnologia e os dados dos clientes do Cetelem;
- Informar as áreas e atribuir as responsabilidades para cumprimento desta política e garantia da segurança da informação;
- Dar ciência ao público em geral.

DISPOSIÇÕES GERAIS

Abrangência

Esta política destina-se a todos os colaboradores, parceiros, fornecedores, prestadores de serviços e clientes do Cetelem.

Para os fins do disposto nesta política o termo "colaboradores" abrange todos os empregados, menores aprendizes, estagiários e administradores do Cetelem.

Toda a atividade do Cetelem deve respeitar os princípios estabelecidos nesta política; e tais princípios devem ser aplicados a todos os que estão acima mencionados.

Diretrizes

O Cetelem visa atingir um alto padrão de cibersegurança. Por isso, é comprometido com a confidencialidade, integridade e disponibilidade de todos os ativos físicos e lógicos de informação da empresa, garantindo que os requisitos legais, operacionais e contratuais sejam cumpridos. A preocupação com os riscos cibernéticos é comum aos diversos níveis de gestão e um compromisso individual de todos.

Aspectos gerais

Documento visa estabelecer princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados, garantindo a proteção adequada dos ativos e dos dados, garantindo assim a identificação, proteção, detecção, resposta e recuperação de eventos em casos de eventual incidente de segurança.

Identificação

Desenvolver uma cultura organizacional para gerenciar o risco de cibersegurança, sistemas, pessoas, ativos, dados e capacidades. Além disto, visa realizar o registro, análise de causa e impacto, e controle dos efeitos de incidentes, incluindo informações recebidas de terceiros, utilizando como base os seguintes processos e recursos, a fim de mitigar riscos:

- Regulamentações vigentes;
- Diretrizes e normas do Banco Central do Brasil;
- Gerenciamento de ativos;
- Ambiente de negócios;
- Governança;
- Avaliação de risco;
- Estratégia de gerenciamento de riscos;

Proteção

Desenvolver e implementar salvaguardas apropriadas para garantir o controle e a mitigação de riscos, incluindo, mas não se limitando a realização de:

- Controle de acesso;
- Conscientização e treinamentos; e
- Processos e procedimentos para proteção das informações.

Detecção

Desenvolver e implementar ações estruturadas para identificar a ocorrência de eventuais eventos que causem riscos e comprometam a cibersegurança, incluindo, mas não se limitando a:

- Monitoramento de eventos e anomalias;
- Monitoramento contínuo de segurança, incluindo parceiros, fornecedores, prestadores de serviços e clientes;
- Processo de detecção, análise e mitigação de riscos;
- Plano de resposta a incidentes;
- Comunicação; e
- Monitoramento e melhoria contínua

RESPONSABILIDADES

Dos colaboradores, parceiros, fornecedores, prestadores de serviços e clientes:

- Salvaguardar todo recurso e informação das empresas componentes do Cetelem criada ou utilizada nas suas atividades, inclusive, mas não se limitando a distribuição não autorizada, acesso indevido, modificação ou destruição;
- Conhecer suas responsabilidades a respeito da cibersegurança, atuando de forma segura, ética e legal na utilização dos recursos e dados, primando pela preservação da integridade, confidencialidade e disponibilidade das informações da empresa;
- Relatar ao CSIRT através do e-mail csirt@cetelem.com.br qualquer situação que represente desvio ou violação desta Política bem como das normas vigentes.
- A área de cibersegurança é responsável por manter e atualizar esta política.

MEDIDAS DISCIPLINARES

As violações a esta política estão sujeitas às ações disciplinares previstas nas normas internas do Cetelem e na legislação brasileira vigente.

REFERÊNCIAS

- 1-DTI.23 – Política de Cibersegurança
- Resolução 4893 do Banco Central do Brasil
- Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018)
- NIST – Cyber Security Framework

GLOSSÁRIO

CSIRT: CSIRT é o acrônimo de *Computer Security Incident Response Team*, ou seja, Grupo de Resposta e Tratamento a Incidentes de Segurança da Informação e tem como responsabilidade receber, analisar, tratar (quando aplicável) e responder às notificações e atividades relacionadas aos incidentes de segurança da informação envolvendo a Cetelem.

NIST: NIST é o acrônimo de *National Institute of Standards and Technology*. É uma agência governamental não regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos. A missão do instituto é promover a inovação e a competitividade industrial dos Estados Unidos, promovendo a metrologia, os padrões e a tecnologia de forma que ampliem a segurança econômica e melhorem a qualidade de vida.