Política

Versão	Data de publicação	Área(s) responsável (is)	Classificação	Código
01.2019	DD/MM/AAAA	TI – Segurança da Informação	Pública	1-SXXXX00.00

POLÍTICA DE CIBERSEGURANÇA DO BANCO CETELEM S.A. ("CETELEM")

Política

ÍNDICE

1. OBJETIVO 3
2. DISPOSIÇÕES GERAIS 3
   - 2.1 Abrangência 3
   - 2.2 Diretrizes 3
   - 2.3 Aspectos Gerais 3
   - 2.3.1 Identificação 3
   - 2.3.2 Proteção 4
   - 2.3.3 Detecção 4
   - 2.3.4 Recuperação 4
3. RESPONSABILIDADES 4
   - 3.1 Colaboradores, Parceiros, fornecedores, prestadores de serviços e clientes 4
4. MEDIDAS DISCIPLINARES 4
5. REFERÊNCIAS 5
6. GLOSSÁRIO 5
7. ÁREA RESPONSÁVEL 5

Política

1. OBJETIVO

Esta 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.

2. DISPOSIÇÕES GERAIS

2.1 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.

2.2 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.

2.3 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.

2.3.1 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

2.3.2 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.

2.3.3 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.

2.3.4 Recuperação

Desenvolver e programar ações sustentáveis para manter os planos de resiliência e restaurar quaisquer recursos ou serviços que foram prejudicados devido a um eventual incidente de Cibersegurança, incluindo, mas não se limitando a:

- Comunicação junto aos envolvidos.
- Mapeamento e implementação de melhorias; e
- Plano de recuperação;

3. RESPONSABILIDADES

3.1 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.

4. MEDIDAS DISCIPLINARES

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

5. REFERÊNCIAS

- 1-DTI.23 – Política de Cibersegurança
- Resolução 4658 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

6. 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.

7. ÁREA RESPONSÁVEL

A área de Cibersegurança é responsável por manter e atualizar esta Política.

PUBLICADA NA INTRANET DO CETELEM EM 28/02/2019.