

BANCO
FIBRA

Política de Segurança Cibernética



1. Definição

Este documento descreve diretrizes sobre a Política de Segurança Cibernética do Banco Fibra, cujas regras e procedimentos são de cunho confidencial, publicadas internamente. Tais diretrizes orientam o uso aceitável dos ativos de informação e/ou tecnológicos da instituição, baseada nos princípios de confidencialidade, integridade e disponibilidade.

2. Público alvo

Banco Fibra S.A. e Terceiros Prestadores de Serviço.

3. Objetivo

- Estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores do Banco Fibra adotar padrões de comportamento seguro, adequados às suas metas e necessidades;
- Prevenir possíveis causas de incidentes de segurança cibernética;
- Capacitar os colaboradores Banco Fibra no que se refere à prevenção, detecção e resposta a incidentes de segurança cibernética;
- Orientar os colaboradores quanto a adoção de controles e processos para atendimento dos requisitos de segurança da informação;
- Resguardar ativos de informação e / ou tecnológicos do Banco Fibra, garantindo requisitos de confidencialidade, integridade e disponibilidade;
- Minimizar os riscos de perdas financeiras, da confiança de clientes ou de qualquer outro impacto negativo no negócio do Banco Fibra como resultado de falhas de segurança.

4. Responsabilidades

A Política de Segurança Cibernética do Banco Fibra trata sobre responsabilidades gerais da instituição, de seus colaboradores e terceiros, bem como da Alta Administração.

5. Gestão de Riscos Cibernéticos

A gestão de riscos cibernéticos é uma responsabilidade da área de Segurança da Informação. Este processo identifica os requisitos de segurança relacionado às necessidades da instituição. A gestão de riscos cibernéticos é contínua e define contextos internos e externos para avaliação, além de tratar dos riscos identificados de modo que sejam reduzidos à níveis aceitáveis.

6. Uso Aceitável de Recursos Tecnológicos

Os recursos de tecnologia do Banco Fibra devem ser utilizados de forma profissional, ética e legal, conforme definido no termo de responsabilidade aplicável.

A Política de Segurança Cibernética aborda a definição de recursos tecnológicos, além de regras que tratam deste tema, pelas quais os colaboradores e terceiros do Banco devem seguir.

7. Conscientização e Treinamentos de Segurança da Informação

O Banco Fibra define diretrizes de educação contínua para aculturação de boas práticas de segurança e disseminação de conhecimento para utilização no dia-a-dia dos colaboradores, seja para fins profissionais quanto para fins pessoais. A Política aborda procedimentos utilizados no programa de conscientização da instituição, tais como treinamentos e informativos internos.

8. Proteção e Classificação de Dados

O Banco Fibra estabelece diretrizes para a classificação, manuseio e rotulagem dos ativos de informação da instituição. O documento interno prevê todas as diretrizes utilizadas para a classificação da informação, descreve suas categorias, prevê ainda diretrizes para o manuseio da informação, para o descarte da informação, descreve regras sobre prevenção a vazamento de dados (DLP) e políticas, sobre cópia e restauração de dados (*backup e restore*), bem como sobre criptografia.

9. Proteção Contra Códigos Maliciosos

O Banco Fibra define diretrizes para proteção contra ameaças de códigos maliciosos (*“malwares”*).

10. Gestão de Vulnerabilidade e Conformidade

O Banco Fibra possui processos de gestão de vulnerabilidades e conformidade, de modo que as seguintes diretrizes estão estabelecidas:

- Gestão de Vulnerabilidade;
- Gestão de Conformidade;
- Correções de Segurança (*Patch Management*); e
- Testes Periódicos de Segurança.

11. Monitoramento de Segurança

A Política de Segurança Cibernética trata sobre o monitoramento de segurança, descrevendo os aspectos necessários para identificação de eventuais ameaças.

12. Respostas a Incidentes de Segurança Cibernética

O Banco Fibra define diretrizes para prevenir, responder e tratar adequadamente incidentes de segurança cibernética que estejam impactando ou possam vir a impactar ativos/serviços de informação ou recursos tecnológicos da instituição.

Neste tópico, a Política trata sobre responsabilidades das áreas na prevenção e resposta a incidentes.

Além disso, a Política descreve regras de priorização e severidade com relação a possíveis incidentes, procedimentos sobre a definição de autoridades e regras para a elaboração de cenários de testes de continuidade de negócio.

Cabe ainda ressaltar que o Banco Fibra possui Plano de Prevenção e Resposta a Incidentes, contendo metodologia e diretrizes para tratamento de incidentes de segurança cibernética.

13. Gestão de Terceiros

O Banco Fibra estabelece diretrizes para profissionais terceiros em suas dependências ou para contratação de serviços.

O Banco possui regras de diligência adicionais para terceiros considerados relevantes, que são aqueles que armazenem ou processem dados considerados críticos em estrutura tecnológica não pertencente ao Banco Fibra.

14. Gestão de Continuidade de Negócios

O Banco Fibra realiza a gestão de continuidade de negócios com soluções, estratégias e procedimentos a serem executados durante eventuais cenários de contingência alinhados com o propósito e metas estratégicas da instituição. Para tal, o Banco Fibra possui um Plano de Continuidade de Negócios (PCN) que cumpre funções definidas em documento interno.

15. Gestão de Identidade de Acessos

A instituição estabelece diretrizes gerais para acesso a ativos e sistemas de informação. Toda gestão de acessos é responsabilidade da área de Segurança da Informação e é baseada no princípio da necessidade de acesso à informação para a execução das atividades laborais do colaborador (princípios *need to know*, e *least privilege*).

A Política define diretrizes, tais como:

- Perfis de Acesso das Áreas de Negócio;
- Processo de Admissão ou Transferência de Área de Colaboradores;
- Processo de Desligamento de Colaboradores;
- Acesso de Terceiros e/ou Temporários;
- Acesso a Banco de Dados;
- Utilização de Conta Administrativa na Rede Corporativa;
- Acesso Remoto;
- Acesso Físico;
- Revisão de Acessos;
- Parametização de Senhas; e
- Autenticação.

16. Segurança de Dispositivos Móveis

O Banco Fibra define diretrizes para utilização segura de dispositivos móveis, bem como as atribuições das áreas responsáveis pelo monitoramento.

17. Segurança em Sistemas e Aplicações

Todos os sistemas ou aplicações, sejam eles desenvolvidos internamente ou adquiridos de terceiros devem seguir diretrizes definidas na Política de Segurança Cibernética.

18. Segurança em Redes

O Banco Fibra possui ferramentas de segurança capazes de detectar e responder tentativas de intrusão em seu ambiente de rede, considerando o ambiente de nuvem e local. No presente tópico, a Política aborda, também, regras sobre a rede Wi-Fi corporativa e pública.

19. Sanções e Punições

A área de Segurança da Informação realiza o monitoramento contínuo do ambiente tecnológico por meio de métodos diversos para assegurar a conformidade e adesão a esta Política. Caso haja violação das regras nela dispostas, bem como às demais normas e procedimentos de Segurança da Informação, mesmo que por omissão ou tentativa não consumada, tal violação pode ser classificada como incidente de segurança cibernética, os quais são passíveis de penalidades.

As demais sanções e punições para o descumprimento das regras de Segurança da Informação estão descritas na Política interna.