Política de Segurança Cibernética

Publicada em 30/04/2026

BANCO FIBRA

Política de Segurança Cibernética

Data base: 2026

BANCO FIBRA

Objetivo da Política

A Política de Segurança Cibernética tem como objetivo estabelecer diretrizes de segurança da informação e segurança cibernética para orientar os colaboradores na adoção de comportamentos seguros, visando à proteção dos ativos de informação e tecnologia garantindo confidencialidade, integridade e disponibilidade.

Público-alvo

Esta política aplica se a todos os colaboradores, terceirizados, fornecedores e demais partes que tenham acesso a informações, sistemas ou recursos tecnológicos do Banco Fibra e de suas controladas.

Responsabilidades

Área de Segurança da Informação:

- Elaborar, implantar, disponibilizar e atender as políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos de confidencialidade, integridade e disponibilidade da informação sejam atingidos por meio de adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas;
- Garantir a conscientização dos colaboradores sobre as melhores práticas de segurança da informação;
- Atender requisitos de segurança da informação aplicáveis ou exigidos pela regulação vigente bem como por cláusulas contratuais;
- Tratar incidentes de segurança cibernética, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicar as autoridades competentes;
- Melhorar continuamente a gestão de segurança da informação por meio de definição e revisão sistemática de objetivos de segurança em todos os níveis da instituição.

Responsabilidades

Colaboradores e Terceiros

- Seguir as diretrizes desta política e normativos de Segurança da Informação, assim como as orientações transmitidas pela área de Segurança da Informação;

Tecnologia da Informação

- Garantir a geração de evidências técnicas para suportar auditoria rastreabilidade;
- Executar atividades técnicas e implementar controles necessários para corrigir, mitigar e identificar vulnerabilidades;

Alta Administração

- Patrocinar e apoiar a Segurança Cibernética, assegurando o compromisso institucional com a melhoria contínua dos controles e da cultura de Segurança da Informação.
- Garantir a efetiva implementação da Política, promovendo sua comunicação, entendimento e cumprimento em todos os níveis da organização.
- Estimular a conscientização e a resiliência organizacional, apoiando ações de treinamento, aprimoramento de processos, exercícios de continuidade de negócios e a manutenção de informações críticas atualizadas.

Gestão de Riscos Cibernéticos

A instituição mantém um processo contínuo de gestão de riscos cibernéticos, voltado à identificação, avaliação e tratamento de riscos que possam impactar informações, sistemas e a continuidade das operações. Esse processo considera fatores internos e externos e visa manter os riscos em níveis aceitáveis, alinhados às necessidades do negócio.

Conscientização e Treinamentos de Segurança da Informação

São definidas diretrizes de educação contínua para aculturamento 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.

Gestão de Vulnerabilidade e Conformidade

São estabelecidos processos estruturados de gestão de vulnerabilidades e não conformidades, com o objetivo de garantir sua identificação e remediação em tempo adequado definido por SLA acordado com TI, assegurando a aderência às regulamentações e aos padrões de segurança relevantes.

Monitoramento, Prevenção e Detecção de Intrusão

O Banco Fibra estabelece e mantém ferramentas, processos e procedimentos definidos para o monitoramento contínuo das atividades e eventos em seus sistemas e redes, com o objetivo de identificar e responder de forma tempestiva a potenciais ameaças à segurança, violações de políticas ou incidentes de segurança cibernética, assegurando a detecção precoce de atividades maliciosas.

Criptografia

O uso de criptografia é aplicado como prática essencial para proteger informações sensíveis, tanto em trânsito quanto em repouso. Essa medida contribui para garantir a confidencialidade, a integridade e a autenticidade dos dados tratados pelo banco.

Gestão de Identidades e Controle de Acessos

São adotados controles para garantir que o acesso a sistemas, redes e informações seja concedido somente a usuários devidamente autorizados, conforme a necessidade para execução de suas atividades. Esses controles contribuem para a proteção das informações e para a redução de acessos indevidos.

Proteção Contra Softwares Maliciosos

O Banco Fibra adota medidas de proteção para prevenir, detectar e mitigar ameaças cibernéticas, incluindo softwares maliciosos e tentativas de acesso não autorizado. Essas práticas visam preservar a integridade dos sistemas e a segurança das informações.

Rastreabilidade

São mantidos mecanismos de registro e rastreabilidade das atividades relevantes nos sistemas, permitindo a identificação de falhas, a análise de eventos de segurança e o suporte a investigações, quando necessário, sempre de forma alinhada às diretrizes internas.

Gestão de Cópias de Segurança dos Dados e das Informações

O Banco Fibra mantém práticas de backup e recuperação de dados com o objetivo de proteger informações críticas e assegurar a recuperação das operações em caso de incidentes ou falhas, contribuindo para a disponibilidade e a resiliência dos serviços.

Gestão de Certificados Digitais

A segurança das comunicações institucionais é sustentada por práticas estruturadas de gestão de certificados digitais, que abrangem todas as etapas do seu uso ao longo do tempo, assegurando controle, rastreabilidade e confiabilidade dos certificados empregados nos sistemas e processos do Banco Fibra.

Perfis de Configuração Segura de Ativos de Tecnologia

São estabelecidos padrões de configuração segura para os ativos tecnológicos, com o objetivo de minimizar riscos de segurança cibernética. Essas práticas incluem monitoramento contínuo e correção de desvios, assegurando a proteção e a conformidade dos sistemas ao longo de seu uso.

Mecanismos de Proteção de Rede

Para fortalecer a segurança da rede, a segmentação dos ambientes é adotada como prática essencial, reduzindo a superfície de ataque e limitando a propagação de ameaças, especialmente em ambientes de produção e em recursos que suportam processos críticos de negócio.

Resposta a Incidentes de Segurança Cibernética

São estabelecidas diretrizes para a prevenção, o tratamento e a resposta a incidentes de Segurança Cibernética, com foco na proteção de ativos, serviços de informação e recursos tecnológicos. Esses incidentes são devidamente registrados e analisados, considerando suas causas e impactos, de forma a controlar seus efeitos e apoiar ações adequadas de resposta e melhoria contínua.

Segurança na Integração de Sistemas de Informação

São adotadas diretrizes de segurança para integrações entre sistemas, garantindo controles de acesso, autenticação adequada e proteção dos dados. A segurança dessas interfaces é continuamente avaliada por meio de monitoramento e análises técnicas, permitindo a identificação e mitigação de vulnerabilidades e riscos, assegurando a confiabilidade das comunicações entre sistemas.

Ações de Inteligência no Ambiente Cibernético

É mantido um processo contínuo de inteligência cibernética com foco na identificação, análise e reporte de informações relevantes para a proteção de ativos, dados, pessoas, marca e continuidade dos negócios. Esse processo inclui o monitoramento de ambientes digitais, como internet pública e, quando aplicável, outros ambientes online, com o objetivo de identificar ameaças emergentes, tentativas de fraude ou exposição indevida de informações, permitindo a atuação preventiva e a resposta adequada.

Gestão do Acesso Físico

A gestão de acesso físico às dependências do Banco Fibra, Filial Cayman e de suas controladas é realizada por meio de diretrizes que asseguram a identificação e o controle de colaboradores, terceiros e visitantes, incluindo o uso obrigatório de crachás pessoais e intransferíveis, contribuindo para a proteção das pessoas e das instalações da instituição.

Gestão de Continuidade de Negócios

A gestão de continuidade de negócios é realizada por meio de estratégias e procedimentos alinhados aos objetivos da instituição, com suporte de um Plano de Continuidade de Negócios que identifica processos críticos, avalia riscos e impactos, orienta a resposta a incidentes e contingências, minimiza efeitos sobre partes interessadas e patrimônio, preserva a reputação institucional, promove o preparo das equipes envolvidas e assegura o atendimento aos requisitos regulatórios aplicáveis.

Gestão de Riscos de Segurança de Fornecedores

A gestão de riscos de Segurança da Informação e Segurança Cibernética aplicável a fornecedores tem como objetivo mitigar impactos aos dados, sistemas e à continuidade dos negócios, assegurando que terceiros não representem riscos indevidos ao ambiente do Banco Fibra, Filial Cayman e de suas controladas, sendo aplicada prioritariamente a fornecedores com maior nível de acesso a informações ou recursos tecnológicos, conforme critérios internos de criticidade, confidencialidade, disponibilidade e continuidade operacional.