BANCO FIBRA

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Versão 15 - Mar/23

1. DEFINIÇÃO

A política de Segurança Cibernética descreve o conjunto de diretrizes que orientam o uso aceitável dos ativos de informação e/ou tecnológicos, baseada nos princípios de confidencialidade, integridade e disponibilidade.

2. PÚBLICO-ALVO

Banco Fibra S.A, suas controladas (“Banco Fibra” ou “Banco”) e Terceiros Prestadores de Serviço.

3. OBJETIVO

Esta política tem por objetivo:

- Estabelecer diretrizes e normas de segurança da informação e segurança cibernética que permitam aos colaboradores adotar padrões de comportamento seguro, adequados às suas metas e necessidades;
- Prevenir possíveis causas de incidentes de segurança cibernética;
- Capacitar os colaboradores 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 e segurança cibernética;
- Resguardar ativos de informação e/ou tecnológicos, 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 como resultado de falhas de segurança.

4. RESPONSABILIDADES

4.1. RESPONSABILIDADES GERAIS DO BANCO FIBRA

- 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 educação e conscientização sobre as melhores práticas de segurança da informação e segurança cibernética;

- Atender requisitos de segurança da informação e segurança cibernética aplicáveis ou exigidos pela regulação vigente bem como por cláusulas contratuais;
- Tratar incidentes de segurança cibernética, garantindo que sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicar as autoridades competentes;
- Garantir a continuidade dos negócios através da melhoria contínua de planos de continuidade; e
- 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.

4.2. RESPONSABILIDADES DOS COLABORADORES E TERCEIROS

- Seguir as políticas, padrões e procedimentos para o cumprimento das diretrizes desta política, assim como as orientações transmitidas pela área de Segurança da Informação.

4.3. RESPONSABILIDADES DA ALTA ADMINISTRAÇÃO

- Comprometer-se com a melhoria contínua dos procedimentos relacionados à segurança da informação e segurança cibernética, assim como com a disseminação da cultura de segurança da informação;
- Adotar medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da instituição; e
- O Diretor responsável por Segurança da Informação e Cibernética é responsável pelo devido cumprimento desta política e pela execução do Plano de Prevenção e Resposta a Incidentes.

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 relacionados 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.

Segurança da Informação

- Deve reportar ao Comitê Executivo do Banco Fibra, quando necessário, os riscos cibernéticos identificados, assim como buscar alternativas para a mitigação; e
- Deve manter atualizado os procedimentos operacionais da área em ambiente controlado.

Alta Administração

- Na impossibilidade de mitigação do risco cibernético, uma avaliação deve ser realizada pelo Comitê Executivo e a decisão documentada através de “carta de aceitação”, se for o caso.

6. USO ACEITÁVEL DE RECURSOS TECNOLÓGICOS

Os recursos de tecnologia devem ser utilizados de forma profissional, ética e legal, conforme definido no termo de responsabilidade denominado “Termo de Responsabilidade Sobre o uso de Bens de Tecnologia”.

São exemplos de recursos de tecnologia notebooks, computadores, celulares e tablets corporativos, e-mail corporativo, internet, rede de computadores, dentre outros. Desta forma, o Banco Fibra define as seguintes diretrizes para a adequada utilização destes:

Colaboradores e Terceiros:

- É expressamente proibida a execução de qualquer atividade potencialmente maliciosa ou que objetive exploração de vulnerabilidades, interceptação de dados ou tráfego de rede, elevação indevida de privilégios, evasão das camadas de defesa de segurança cibernética, acessos indevidos a credenciais, movimentação lateral, captura, exfiltração indevida de dados, assim como forjar ou simular identidades;
- É expressamente proibido utilizar recursos tecnológicos do Banco Fibra e suas controladas para disseminar ou transmitir mensagens ou dados de caráter injurioso, calunioso, de conteúdo que incite o uso de drogas, terrorismo, práticas subversivas, violência, práticas racistas ou sexuais assim como qualquer outro que possa infringir a legislação vigente, incluindo manifestações políticas ou ideológicas;
- É expressamente proibida a conexão de qualquer equipamento não homologado na rede do Banco Fibra e suas controladas, incluindo dispositivos pessoais;
- É expressamente proibida a instalação de qualquer software não licenciado ou não homologado pela área de Segurança da Informação. Esta verificação de Segurança da Informação tem por objetivo a avaliação de possíveis riscos e vulnerabilidades no software em questão;
- É expressamente proibida a execução de programas ou softwares potencialmente maliciosos (ex.: vírus, *worms*, cavalos de troia etc.);
- Não é permitido que os colaboradores permaneçam como administradores locais de suas estações de trabalho. Exceções devem ser tratadas por meio de ferramenta de elevação de privilégio;

- Não é permitido enviar informação classificada como de “Restrita ao Fibra” para endereços eletrônicos que não façam parte do domínio corporativo do Banco Fibra, Filial Cayman e suas controladas, excetuando-se quando expressamente autorizados;
- Não é permitido o armazenamento local nas estações de trabalho de documentos, arquivos ou papéis de trabalho em desenvolvimento ou concluído, dado a impossibilidade técnica de execução de backup (ex.: disco rígido local). Para armazenamento destes documentos deve-se utilizar as soluções de armazenamento corporativo homologadas. Somente os diretórios “Meus Documentos”, “Área de Trabalho” e “Imagens” possuem backup automático.
- Documentos departamentais devem ser salvos sempre na rede corporativa. Documentos em fase de desenvolvimento podem ser armazenados no Microsoft OneDrive;
- Não é permitido o uso de qualquer outra solução de armazenamento na nuvem, que não seja a oficialmente adotada pela empresa e homologada pela área de Segurança da Informação do Banco Fibra (Microsoft OneDrive);
- O bloqueio de tela deve ser ativado imediatamente pelo colaborador sempre que se afastar da estação de trabalho que estiver utilizando;
- A área de Tecnologia da Informação deve realizar configuração através de políticas de grupo para garantir o bloqueio automático de tela em estações de trabalho após 10 minutos de inatividade;
- O Banco Fibra fornece o serviço de e-mail para seus colaboradores para o desempenho de suas atividades profissionais. É vedada a utilização de qualquer serviço de mensageria não homologada para qualquer tipo de formalizações de cunho corporativo (ex.: novos negócios, contratação de fornecedores, dentre outras);
- O colaborador deve retirar imediatamente da impressora ou fotocopiadora os documentos que tenha solicitado a impressão, transmissão ou cópia que contenham informações classificadas como de “Restrito” ou “Restrito ao Fibra”, conforme diretrizes de Proteção e Classificação de Dados definidas neste documento;
- Documentos físicos não utilizados (ex.: papéis, CDs, DVDs, discos rígidos etc.) com informações internas ou confidenciais devem ser destruídos ou armazenados em local seguro imediatamente, conforme diretrizes sobre Proteção de Dados deste documento;
- Os recursos tecnológicos do Banco Fibra e suas controladas, inclusive serviços de e-mail, são continuamente monitorados. Este monitoramento objetiva proteger a instituição, atestar o respeito às regras contidas neste documento, bem como produzir evidências relativas a eventuais violações das mesmas e/ou legislação em vigor. O Banco Fibra e suas controladas se resguardam ao direito de, sem qualquer notificação ou aviso, monitorar, interceptar, registrar, ler, bloquear, redirecionar, retransmitir, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais todos os dados enviados ou recebidos pelos colaboradores através de sua infraestrutura de TI.

7. CONSCIENTIZAÇÃO E TREINAMENTOS DE SEGURANÇA DA INFORMAÇÃO

O Banco Fibra define 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.

8. PROTEÇÃO E CLASSIFICAÇÃO DE DADOS

O Banco Fibra estabelece diretrizes para (i) classificação das informações; (ii) manuseio das informações; (iii) descarte das informações; (iv) prevenção a vazamento de dados (DLP); (v) cópia e restauração de dados (*backup e restore*); (vi) criptografia; e (vii) mascaramento de dados dos ativos de informação da instituição.

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 abaixo relacionadas estejam estabelecidas:

- Gestão de Vulnerabilidade;
- Gestão de Conformidade;
- Grupo de Trabalho de Vulnerabilidades;
- Correções de Segurança (Patch Management e SLA para Correção de Vulnerabilidades); 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 em sua Política 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.

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, em conformidade com a regulamentação e autorregulamentação aplicáveis em vigor.

13. GESTÃO DE TERCEIROS

O Banco Fibra possui regras de diligência adicional 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, Filial Cayman e suas controladas possuem um Plano de Continuidade de Negócios (PCN) que cumpre funções definidas em documento interno.

15. GESTÃO DE IDENTIDADE DE ACESSOS

O Banco Fibra estabelece diretrizes definidas para gestão de identidades e acessos. Toda gestão de acessos a sistemas corporativos produtivos, pastas de rede em *file share* ou a servidores (acessos interativos) é de 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:

- Acesso de Ativos e sistemas de informação;
- Acesso a Sistemas ou Diretórios de Rede;
- 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;

- Parametrização de Senhas;
- Autenticação; e
- Autenticação do Cliente.

16. SEGURANÇA EM 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. SEGURANÇAS 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 à Política de Segurança Cibernética.

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.

Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em danos ao Banco Fibra, Filial Cayman e suas controladas o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos na Política de Segurança Cibernética.