Política Específica de Gsegurança da Informação e Cibernética

Regulamentação: Decreto 9.637/2018, Resoluções 4.557/2017 e 4.893/2021 do Conselho Monetário Nacional e Resolução 85/21 do Banco Central do Brasil. Essa política está em conformidade com a Resolução 304/23 do Banco Central do Brasil.

Periodicidade de revisão: no mínimo anualmente, ou, extraordinariamente, a qualquer tempo.

Introdução e Conceitos

Esta Política orienta o comportamento da ABFunding.

Esta política estabelece diretrizes aplicadas à gestão da segurança da informação e cibernética, demonstrando o compromisso do Banco com a proteção das informações corporativas e demais ativos de informação. Ela compõe a relação de políticas associadas ao gerenciamento do risco operacional do Banco ABF.

Os critérios, requisitos, normas e procedimentos decorrentes da presente Política estão definidos em instruções normativas internas (IN).

Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

Ciclo de vida da informação: são as fases da criação, processamento, armazenamento, transmissão, exclusão e destruição da informação.

Tratamento da Informação: conjunto de ações e controles que, aplicados, têm o objetivo de proteger as informações durante todo o seu ciclo de vida independentemente do meio em que se encontra (físico ou lógico.

Segurança Cibernética: estrutura constituída por diretrizes, processos, pessoas e ferramentas organizados de forma integrada para defesa e resposta contra ameaças, vulnerabilidades e ataques intencionais internos e externos, baseados em Tecnologia da Informação (TI), com potencial para impactar diretamente a confidencialidade, integridade e disponibilidade de sistemas que suportam os negócios do Banco.

Segurança da Informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

Enunciados:

Tratamos a informação, na gestão empresarial, como ativo.

Alinhamos a gestão da segurança da informação e cibernética aos nossos negócios.

Realizamos o tratamento da informação em todo o seu ciclo de vida de modo ético e responsável.

Garantimos a confidencialidade, integridade e disponibilidade da informação em todo o seu ciclo de vida: produção, manuseio, reprodução, transporte, transmissão, armazenamento e descarte.

Aplicamos proteção aos ativos de informação de forma compatível com sua criticidade para

nossas atividades, alcançando todos os processos, informatizados ou não, inclusive quando do uso de computação em nuvem.
Identificamos, analisamos, avaliamos e tratamos os riscos que envolvam os ativos de informação, por meio de avaliações periódicas, a intervalos regulares.

Adotamos mecanismos de proteção contra uso indevido, fraudes, danos, perdas, erros, sabotagens, e roubo e ataques cibernéticos, em todo o ciclo de vida das informações.

Monitoramos de forma contínua os ativos de informação e utilizamos processos, controles e tecnologias de prevenção e resposta a ataques cibernéticos.

Obedecemos ao princípio de segregação das funções de desenvolvimento e uso dos ativos da informação, na gestão da segurança da informação e cibernética.

Procedemos à identificação e definição de, pelo menos, um gestor da informação e atribuímos-lhe responsabilidades sobre a informação em todo o seu ciclo de vida.

Disseminamos a cultura de segurança da informação e cibernética por meio de programa permanente de sensibilização, conscientização e capacitação.

Preservamos nossos requisitos de segurança da informação e cibernética na contratação de serviços ou de pessoas e no relacionamento com colaboradores, fornecedores, terceiros, parceiros, contratados e estagiários.

Concedemos a funcionários e a terceiros somente o acesso às informações necessárias ao desempenho de suas funções e atribuições previstas em contrato ou por determinação legal.

Identificamos, por meio do controle de acesso, cada usuário individualmente e nos casos devidamente comprovados de tratamento indevido da informação corporativa o responsabilizamos, juntamente com o administrador que lhe concedeu o acesso.

Analisamos as ocorrências de tratamento indevido de informações corporativas sob os aspectos legal e disciplinar, imputando responsabilização, e sob o aspecto técnico, corrigindo as vulnerabilidades.

Esta Política foi aprovada pelo Conselho de Administração em reunião de 30.12.2024.