FUNDAÇÃO BB

Política de Segurança da Informação e Cibernética

1. Área responsável pelo assunto:

Gerência de Controles, Riscos e Integridade (Gecri).

2. Periodicidade de revisão:

Ordinariamente, na reunião do Conselho Curador (CC) seguinte à aprovação do Plano Estratégico para novo período e pelo menos uma vez durante a vigência do Plano, ou extraordinariamente, a qualquer tempo.

3. Abrangência:

Esta Política orienta o comportamento da Fundação Banco do Brasil (Fundação BB).

4. Regulamentação:

4.1. Normas legais: Lei 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD).

4.2. Normas Infralegais e Melhores Práticas: ABNT NBR ISO/IEC 27014:2021 Segurança da Informação e Cibernética e Proteção da Privacidade.

5. Introdução e Conceitos:

Esta Política orienta a Fundação BB na gestão da segurança da informação e cibernética, demonstrando nosso compromisso com a proteção das informações corporativas e demais ativos de informação.

5.1. Para fins desta Política, são considerados os seguintes conceitos:

5.1.1. **Ativos:** qualquer bem, tangível ou intangível, que tenha valor para a organização.

5.1.2. **Ativos de informação:** os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

5.1.3. **Ciclo de vida da informação:** compreende as fases da informação, que são a produção, o manuseio, a reprodução, o transporte, a transmissão, o armazenamento e o descarte.

5.1.4. **Confidencialidade:** garantia de que a informação não está disponível ou é revelada a usuário não autorizado.

5.1.5. **Integridade:** garantia de que a informação não sofra alterações indevidas, não autorizadas ou acidentais, mantendo sua completeza.

5.1.6. **Disponibilidade:** propriedade de ser acessível e utilizável por um usuário autorizado.

5.1.7. **Princípio de segregação das funções:** consiste na separação de atribuições ou responsabilidades entre diferentes pessoas, especialmente as funções ou atividades-chave de autorização, execução, aprovação, registro e revisão ou auditoria.

5.1.8. **Gestor da informação:** área responsável pela gestão da informação (em suas diversas formas - impressa, escrita, em meio eletrônico, entre outros), durante todo o seu ciclo de vida, dentro do escopo de suas atribuições e/ou responsabilidades.

5.1.9. **Requisitos de segurança da informação:** preservação da confidencialidade, integridade, e disponibilidade das informações.

5.1.10. **Terceiros:** aqueles que não pertencem ao quadro funcional ativo da Fundação Banco do Brasil e que, por interesse do serviço e previsão contratual ou imposição legal, estabeleça relacionamento com a Fundação BB.

6. Enunciados:

6.1. Tratamos a informação, na gestão organizacional, como ativo.

6.2. Aplicamos proteção aos ativos de forma compatível com sua criticidade para nossas atividades, alcançando todos os processos, informatizados ou não, inclusive quando do uso de computação em nuvem.

6.3. Alinhamos a gestão da segurança da informação e cibernética as nossas atividades.

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

6.5. Garantimos a confidencialidade, integridade e disponibilidade da informação em todo o seu ciclo devida.

6.6. Identificamos, analisamos, avaliamos e tratamos os riscos que envolvam os ativos de informação, por meio de avaliações periódicas, a intervalos regulares.

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

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

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

6.10. 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.

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

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

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

6.14. Identificamos, por meio do controle de acesso, cada usuário individualmente e, nos casos devidamente comprovados de tratamento indevido da informação

institucional, o responsabilizamos, juntamente com o administrador que lhe concedeu o acesso.

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

Data da última revisão: 17.12.2024.