FUNDAÇÃO

Política de Segurança da Informação

1. **Área responsável pelo conteúdo e atualização:** Comissão de Segurança da Informação e Continuidade de Negócios, coordenada pela Gerência de Pessoas e Infraestrutura (Gepin).

2. **Periodicidade de revisão:** Concomitante à construção ou revisão dos Planos Estratégicos ou, extraordinariamente, a qualquer tempo.

3. **Abrangência:** Esta política orienta o comportamento da Fundação Banco do Brasil.

4. **Regulamentação:** Normas Complementares nº 02/IN01/DSIC/GSIPR de 13.10.2008 e nº 04/IN01/DSIC/GSIPR de 15.02.2013, publicadas pelo Gabinete de Segurança Institucional da Presidência da República.

5. **Introdução:** Esta política orienta a Fundação Banco do Brasil na gestão da segurança da informação, demonstrando nosso compromisso com a proteção das informações e demais ativos.

5.1. **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 FBB.

6. **Diretrizes:**

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

6.2. Aplicamos proteção a esses ativos de forma compatível com sua criticidade, alcançando todos os processos, informatizados ou não.

6.3. Alinhamos a Gestão da Segurança da Informação aos objetivos estratégicos da Fundação Banco do Brasil.

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 de vida.

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

6.9. 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.

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

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

6.12. 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.

6.13. 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.

6.14. 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.

6.15. Evitamos perdas financeiras e danos à imagem da Fundação, de seu Instituidor e de seus parceiros estratégicos.

7. **Responsabilidades**:

7.1. **Do usuário da Informação:**

7.1.1. A observância e o zelo pelo cumprimento desta Política e das normas relacionadas é responsabilidade de todos os colaboradores e terceiros, sendo obrigação de todo usuário informar ao seu superior imediato quando informações, aplicações ou ativos considerados restritos ou confidenciais forem encontrados sem o tratamento de segurança correto.

7.2. **Do custodiante da Informação:**

7.2.1. Responsável pela guarda adequada da informação, que cuida do ativo onde está armazenada a informação no dia-a-dia, garantindo a integridade, confidencialidade, disponibilidade, boas condições e proteção do ambiente onde estão os recursos que contém a informação.

7.3. **Do Gestor da Informação:**

7.3.1. Cada gestor deverá manter os processos sob sua responsabilidade aderente às políticas, normas e procedimentos específicos de segurança da informação, sendo diligentes com tal responsabilidade.

Data da última revisão*:* 19.12.2018.