#pública

POLÍTICA ESPECÍFICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA*

1. Área Responsável

1.1. Gerência Executiva de Gestão de Riscos.

2. Abrangência

2.1. Esta Política Específica de Segurança da Informação e Cibernética ("Política") orienta o comportamento da BB Gestão de Recursos DTVM (BB DTVM).

3. Regulamentação

3.1. A presente Política tem como principais referenciais normativos:

- Resoluções n.º 4.557/2017 e 4.658/2018, do Conselho Monetário Nacional.
- Política de Segurança Cibernética do Banco do Brasil S.A. de janeiro de 2020.

4. Periodicidade de Revisão

4.1. Esta Política deverá ser revisada no mínimo a cada ano ou, extraordinariamente, a qualquer tempo – observando eventuais alterações legais, normativas ou estatutárias, e revisões da Política Específica de Segurança da Informação e Cibernética do Banco do Brasil S.A.(Controlador) – sendo submetida às instâncias competentes, conforme previsão estatutária, para deliberação.

5. Introdução

5.1. Esta Política orienta a gestão da segurança da informação e cibernética na BB DTVM, demonstrando o compromisso desta Gestora com a proteção das informações corporativas e compondo a relação de políticas associadas ao gerenciamento do risco operacional da BB DTVM.

6. Objetivos

6.1. Reduzir as vulnerabilidades da instituição a ameaças à segurança da informação e prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

7. Enunciados

7.1. Compartilhamos a utilização da infraestrutura tecnológica do Banco do Brasil (BB) – sistemas de Informática e de Comunicações - conforme estabelecido no Estatuto da BB DTVM e no Convênio de Rateio e Despesas firmado entre esta e o Controlador.

7.2. Tratamos a informação como um ativo para a Empresa.

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

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

7.5. Aplicamos na gestão da segurança da informação e cibernética o conjunto de normativos, processos e ações que visem garantir a confidencialidade, integridade e disponibilidade da informação nas fases de produção, manuseio, reprodução, armazenamento, transporte, transmissão e descarte.

7.6. Estabelecemos estrutura de governança para gestão da segurança da informação e cibernética, definindo responsáveis e delimitando as responsabilidades de acordo com a matéria envolvida.

7.7. Aplicamos proteção aos ativos de informação de forma compatível com sua criticidade para nossas atividades, alcançando todos os processos, sejam informatizados ou não.

7.8. Adotamos mecanismos de proteção que visam mitigar a ocorrência de uso indevido, fraudes, danos, perdas, erros, sabotagem, furtos, roubos e ataques cibernéticos em todo o ciclo de vida das informações geradas ou utilizadas pela empresa.

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

7.10. Definimos pelo menos um gestor na administração da informação, imputando-lhe responsabilidades sobre a informação em todo o seu ciclo de vida.

7.11. Estabelecemos critérios de acessos, físicos e lógicos, aos funcionários, estagiários e adolescentes trabalhadores, de acordo com as funções desempenhadas e observadas as determinações legais, quando aplicável.

7.12. Dispomos de critérios de acesso físico aos terceiros contratados.

7.13. Identificamos cada usuário individualmente nos sistemas de controle de acesso, responsabilizando-o, juntamente com o administrador que lhe concedeu o acesso, pelas atividades indevidas, devidamente comprovadas, realizadas sob seu código de identificação.

7.14. Não disponibilizamos informações pessoais relativas à intimidade, vida privada, honra e imagem sem anuência da pessoa a que se referirem, salvo previsão legal ou mediante determinação judicial.

7.15. Apuramos as ocorrências de subtração, violação ou divulgação indevida de informações, nos casos devidamente comprovados, sob os aspectos legal e disciplinar, imputando responsabilização na forma prevista nas instruções normativas do Banco Controlador e/ou da Lei, quando aplicável.

7.16. Aplicamos os quesitos de segurança da informação e cibernética adotados pelo BB na contratação de serviços ou de pessoas e no relacionamento com colaboradores, parceiros, contratados e estagiários.

7.17. Adotamos controles para segurança da informação e cibernética que sejam apropriados à realidade da Empresa e alinhados às práticas adotadas pelo Controlador, tais como programa de mesa e tela limpa, classificação da informação, inventário de informações confidenciais e controles de acesso, físicos e lógicos.

7.18. Identificamos, analisamos, avaliamos e tratamos os riscos que envolvam os ativos de informação, por meio de ações periódicas de autoavaliação, em diferentes camadas de atuação, no sentido de verificar o cumprimento dos requisitos de segurança da informação e cibernética definidos nos normativos, internos e/ou externos.

7.19. Realizamos ações de disseminação de questões sobre segurança da informação e cibernética por meio dos instrumentos e canais internos, como intranet, informativos, e-mail corporativo, e canais externos, como cursos oferecidos na Universidade Corporativa Banco do Brasil.

7.20. Monitoramos, por meio do Controlador, de forma contínua, os ativos de informação abrangidos na infraestrutura de TI provida pelo controlador, os procedimentos, controles e tecnologias para reduzir as vulnerabilidades da instituição a incidentes, atendendo aos objetivos da segurança cibernética.

7.21. Usufruimos do gerenciamento do risco cibernérico realizado pelo Controlador e de sua Política de Segurança Cibernética.

8. Aprovação

8.1. Instância deliberativa competente: Conselho de Administração.

8.2. Data da última revisão: 25.09.2020.