PENTALPHA
bank

PENTALPHA
bank

POLÍTICA ESPECÍFICA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA DO PENTALPHA BANK

1. Área responsável pelo assunto: Unidade Segurança Digital e da Informação.

2. 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.

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

4. Introdução e Conceitos:

4.1. Esta Política orienta o comportamento da PENTALPHA BANK. Espera-se que as Entidades Ligadas ao PENTALPHA BANK definam seus direcionamentos a partir dessas orientações, considerando as necessidades específicas e os aspectos legais e regulamentares a que estão sujeitas.

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

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

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

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

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

4.4.3. 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).

4.4.4. 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 da Instituição.

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

5. Enunciados:

5.1. Tratamos a informação, na gestão empresarial, como ativo.

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

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

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

5.5. Aplicamos proteção aos ativos de informação de forma compatível com sua criticidade para nossas atividades, alcançando todos os processos, inclusive quando do uso e desenvolvimento de modelos e sistemas de inteligência artificial (IA) e de computação em nuvem.

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

5.7. 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.

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

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

5.10. 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.

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

5.12. 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.

5.13. 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.

5.14. 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.

5.15. 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.