PEX.03 - Política Externa de Segurança da Informação e Cibernética

1. Área Responsável: Diretoria de Tecnologia.

2. Aprovação: Diretoria de Tecnologia e Presidência.

3. Abrangência: Esta Política orienta a manutenção da segurança das informações e dos respectivos ativos de informação do Paraná Banco, abrangendo, portanto, todos os ativos conectados à rede corporativa ou rede de provimento de serviços a clientes destas instituições. Também direciona a partir dessas orientações as necessidades específicas e os aspectos legais e regulamentares a que estão sujeitas.

4. Regulamentação Associada: Resolução n° 4.893, de 26/02/2021 do Banco Central do Brasil.

5. Introdução: Esta política orienta o Paraná Banco na gestão da segurança da informação e cibernética, demonstrando o compromisso das instituições com a proteção das informações corporativas e demais ativos de informação. A PEX.03 é derivada da política institucional PIN.19, cuja 7ª versão foi aprovada pelo Conselho de Administração em 26/03/2026.

Em conformidade com a Resolução nº 4.893/2021 do Banco Central do Brasil, esta política também atende à exigência de divulgação ao público de um resumo contendo as linhas gerais da política de segurança cibernética.

6. Diretrizes gerais:

Governança de segurança da informação: elaboração, implementação e observância de políticas, normas e procedimentos que assegurem a confidencialidade, a integridade e a disponibilidade das informações, por meio da adoção de controles voltados à mitigação de ameaças internas e externas.

Atendimento a requisitos de segurança: observância integral das obrigações previstas em regulamentações, legislações aplicáveis e cláusulas contratuais relacionadas à segurança da informação.

Aprimoramento das práticas: evolução contínua da maturidade em segurança da informação com base em boas práticas, frameworks de mercado e padrões reconhecidos no setor financeiro.

Uso adequado de recursos: garantia de que os recursos da instituição não sejam utilizados para práticas que comprometam a segurança das informações próprias ou de terceiros.

Disseminação da cultura de segurança: promoção contínua da conscientização sobre segurança da informação por meio de programas de capacitação, avaliações periódicas e ações de sensibilização dirigidas a colaboradores e demais públicos pertinentes.

Informações a clientes e usuários: disponibilização de orientações sobre precauções na utilização de produtos e serviços, contribuindo para a redução de riscos associados ao uso inadequado.

Observância das regras para processamento e armazenamento de dados e computação em nuvem: adoção dos requisitos regulatórios que asseguram que serviços de processamento, armazenamento e uso de ambientes em nuvem sejam contratados, estruturados e operados com padrões adequados de segurança, contemplando controles previstos pela Resolução CMN nº 4893/2021.

7. Diretrizes técnicas:

Gestão de ativos de tecnologia: definição e manutenção de padrões seguros de configuração, gestão do ciclo de vida com foco em segurança desde a implantação até o descarte, aplicação contínua de correções, adequada configuração de serviços, classificação das informações conforme sensibilidade e garantia de devolução ou desativação de credenciais e dispositivos ao término de vínculos.

Gestão de identidades e acessos: adoção de mecanismos de autenticação robustos, com uso de múltiplos fatores quando aplicável, e implementação de controles que restrinjam o acesso a usuários e dispositivos autorizados, incluindo revisões periódicas das permissões concedidas.

Controles de proteção cibernética: utilização de mecanismos preventivos e detectivos contra ameaças, gestão estruturada de cópias de segurança, e monitoramento contínuo por meio de inteligência cibernética para identificação antecipada de riscos e incidentes.

Segurança de rede e conexões: segmentação de ambientes, aplicação de regras de filtragem e monitoramento de acessos, controle de conexões externas e análise de eventos atípicos, assegurando proteção adequada ao ambiente de produção.

Gestão de vulnerabilidades e riscos: realização de varreduras periódicas, testes de intrusão independentes, correção tempestiva de vulnerabilidades e adoção de medidas proporcionais para tratamento de riscos de segurança da informação.

Gestão de certificados: administração segura de certificados digitais e chaves criptográficas, com monitoramento, rastreabilidade e controle de validade, além de proteção reforçada para certificados utilizados em ambientes críticos como a RSFN.

Segurança aplicacional: incorporação de requisitos de segurança desde a concepção até a operação de sistemas, incluindo desenvolvimento, aquisição e integração, garantindo proteção consistente em todo o ciclo de vida.

Rastreabilidade de transações e operações: geração e retenção de trilhas de auditoria íntegras e protegidas, assegurando a capacidade de monitoramento, análise e identificação de falhas ou anomalias.

Gestão de terceiros: realização de diligências na contratação e monitoramento contínuo de fornecedores, com definição de controles que garantam a proteção de dados e a conformidade com os requisitos de segurança.

Conexão com a RSFN: adoção de controles específicos para comunicação com a rede do Sistema Financeiro Nacional, incluindo autenticação forte, segregação de ambientes, proteção criptográfica, monitoramento de operações, prevenção a fraudes e aderência às normas do Banco Central.

8. Disposições Finais: O Paraná Banco deve certificar-se que suas normas internas estão em conformidade com as disposições desta Política.

A PEX.03 deve ser objeto de avaliação no mínimo anualmente, ou extraordinariamente, a qualquer tempo.

Última aprovação: 26 de março de 2026.