

Política de Segurança da Informação e Cibernética da Vox Instituição de Pagamento (“Vox”).

Este é um resumo contendo as linhas gerais da **Política de Segurança da Informação e Cibernética da Vox**, em cumprimento à Resolução BCB nº 85, de 8 de abril de 2021 do Banco Central do Brasil (“Bacen”).

Versão 2/2026

Sumário

Este documento foi elaborado para atender às exigências da Resolução BCB nº 85/2021, que dispõe sobre a política de cibersegurança e sobre os requisitos para “Serviços Relevantes”, de processamento de dados, armazenamento de dados e de computação em nuvem a serem contratados por instituições financeiras e outras instituições autorizadas a operar pelo Banco Central do Brasil.

Ela exige que tais instituições desenvolvam, implementem e mantenham uma política de Segurança Cibernética abrangente baseada em princípios e diretrizes que buscam garantir a confidencialidade, integridade e disponibilidade dos dados e dos sistemas de informação utilizados.

A política de segurança cibernética deve abranger:

- Objetivos de segurança cibernética, que devem contemplar a capacidade da instituição de prevenir e detectar incidentes cibernéticos, reduzindo a vulnerabilidade;
- Procedimentos e controles para mitigar vulnerabilidades a incidentes e atender a outros objetivos da segurança cibernética, incluindo autenticação, criptografia, prevenção e detecção de intrusão, prevenção de vazamento de dados, realização periódica de testes e varreduras para detecção de vulnerabilidades, proteção contra softwares maliciosos, controle de acesso, redes de computadores segmentadas e manutenção de cópias de segurança dos dados e das informações;
- Controles para garantir a rastreabilidade dos dados, a fim de proteger informações sensíveis;
- Gerenciamento de Incidente, incluindo procedimentos aplicáveis a fornecedores e comunicação tempestiva de incidentes relevantes ao Bacen, incluindo incidentes relatados por fornecedores;
- Cenários de incidentes cibernéticos a serem considerados nos Testes e Planos de Continuidade de Negócios;
- Mecanismos de divulgação da cultura e das disposições da política de segurança cibernética dentro da instituição, incluindo:
 - a) programas recorrentes de treinamento de pessoal;
 - b) informações aos clientes e usuários sobre os cuidados com o uso de produtos e serviços financeiros;
 - c) compromisso da alta administração com a melhoria contínua dos procedimentos relacionados à segurança cibernética.
- Compartilhamento de informações com outras instituições financeiras; e
- Diretrizes para a classificação de dados/informações.

Na Vox, a segurança da informação é um valor essencial. Nossa Política de Segurança Cibernética foi criada para proteger os dados dos nossos clientes, colaboradores, parceiros e fornecedores contra ameaças digitais, garantindo a integridade, a confidencialidade e a disponibilidade das informações.

O que é segurança cibernética?

Segurança cibernética é o conjunto de práticas, tecnologias e processos que protegem nossos sistemas, redes e dados contra acessos não autorizados, ataques, falhas e vazamentos. Na Vox, isso significa proteger você e seus dados em todas as etapas da nossa operação.

Princípios que seguimos

Nossa política é guiada por quatro pilares fundamentais:

- Confidencialidade: apenas pessoas autorizadas acessam as informações.
- Integridade: os dados são mantidos corretos e protegidos contra alterações indevidas.
- Disponibilidade: as informações estão acessíveis sempre que necessário.
- Autenticidade: garantimos que o acesso aos sistemas seja feito por usuários legítimos.

Como protegemos seus dados

Adotamos uma série de medidas técnicas e organizacionais para garantir a segurança:

Controles de acesso

- Cada colaborador tem acesso apenas ao que é necessário para seu trabalho.
- O acesso é protegido por autenticação segura e monitorado continuamente.

Criptografia

- Utilizamos criptografia para proteger dados em trânsito e armazenados, especialmente em redes públicas.

Monitoramento e testes

- Realizamos testes periódicos para identificar vulnerabilidades e corrigir falhas antes que causem danos.

Proteção contra ameaças

- Nossos sistemas contam com antivírus, firewalls e outras ferramentas para prevenir ataques como phishing, malware e ransomware.

Backup e continuidade

- Mantemos cópias de segurança atualizadas e temos planos de continuidade para garantir que os serviços essenciais não sejam interrompidos.

Segmentação de rede

- Isolamos áreas críticas da rede para evitar que um problema em um setor afete toda a operação.

O que fazemos em caso de incidentes

Temos um plano estruturado para lidar com qualquer incidente de segurança:

1. Identificação e contenção da ameaça.
2. Eliminação do problema e recuperação dos sistemas.
3. Análise da causa e melhoria dos processos.
4. Comunicação ao Banco Central, quando necessário.

Também promovemos testes de resposta a incidentes e compartilhamos informações relevantes com outras instituições do setor.

Serviços em nuvem e fornecedores

Ao contratar serviços de terceiros, especialmente de computação em nuvem, exigimos:

- Conformidade com a legislação brasileira.
- Garantia de acesso seguro aos dados.
- Certificações de segurança reconhecidas.
- Capacidade de recuperação e continuidade dos serviços.

Se os serviços forem prestados no exterior, seguimos regras específicas do Banco Central, incluindo comunicação prévia e garantias de acesso aos dados.

Responsabilidades compartilhadas

Todos os colaboradores, parceiros e fornecedores da Vox têm papel ativo na proteção das informações. Por isso, promovemos:

- Treinamentos regulares.
- Campanhas de conscientização.
- Canais de comunicação para reporte de incidentes snoc@voxc cred.com.br