

## **Política de Segurança da Informação e Comunicações e de Segurança Cibernética**

### **OBJETIVO**

Fornecer princípios, diretrizes, critérios e suporte administrativos suficientes à implementação da Segurança da Informação e Comunicações e da Segurança Cibernética, que busquem assegurar a confidencialidade, a integridade e a disponibilidade das informações utilizados pelo Banco.

### **PRINCIPAIS CONCEITOS**

**Ambiente Cibernético:** também denominado de ciberespaço. É qualquer ambiente de comunicação e/ou interconexão de redes de dispositivos digitais interligados, em que não é necessária a presença física humana para constituir a comunicação. Está intrinsecamente, mas não exclusivamente, associado com à *Internet*, e se estende a qualquer ambiente onde ocorra a comunicação entre dispositivos digitais.

**Autenticidade:** garantia da identificação e registro da pessoa que está enviando ou modificando a informação.

**Confidencialidade:** garantia de que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas.

**Disponibilidade:** garantia de que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

**Integridade:** garantia de que as informações sejam mantidas íntegras, sem modificações indevidas - acidentais ou propositais.

**Irretratabilidade:** garantia de que, num processo de envio e recebimento de informações, nenhum participante originador, nem destinatário de informação possa, em um momento posterior, negar a respectiva atuação.

**Segurança da Informação e Comunicações:** conjunto de ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, sejam elas físicas ou digitais.

### **PRINCÍPIOS**

As diretrizes desta Política consideram, prioritariamente, objetivos estratégicos, processos, requisitos legais e estruturais do Banco da Amazônia, além de buscar preservar as informações e seus respectivos ativos quanto à confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade.

### **DIRETRIZES BÁSICAS**

- O ambiente computacional utilizado pelos colaboradores é de exclusiva propriedade do Banco, não podendo ser interpretados como de uso pessoal e serão utilizados apenas para a realização das atividades profissionais.

- Toda informação produzida ou recebida pelos colaboradores, em decorrência da função/cargo exercido e/ou atividade profissional contratada, pertence ao Banco da Amazônia.
- Toda informação de propriedade do Banco é protegida em todo o seu ciclo de vida, sendo utilizada de forma transparente e apenas para a finalidade para a qual foi autorizada.
- O acesso à rede e aos recursos computacionais do Banco é fornecido somente aos colaboradores, cujas credenciais são individuais e seu compartilhamento, vedado.
- O Banco mantém uma estrutura responsável pela Gestão do Risco Operacional de forma consolidada, que participar da identificação, avaliação e mapeamento dos riscos dos novos produtos, atividades, processos e sistemas.
- O Banco mantém um Plano de Continuidade do Negócio, que descreve como manter ou recuperar as operações e assegurar a disponibilidade dos ativos no nível e escala de tempo requerida, com o mínimo de recursos.
- O uso dos recursos de tecnologia da informação, principalmente sistemas que contêm informações sensíveis ou críticas para o Banco, são monitorados e auditados periodicamente.
- O Banco promove um programa contínuo de conscientização e educação em Segurança da Informação e Comunicações (SIC) aos seus colaboradores, parceiros de negócio e clientes, objetivando disseminar boas práticas e fortalecer a maturidade em SIC, de modo a elevar o nível de maturidade e de fortalecimento de postura responsável e consciente.

## **PENALIDADES**

O descumprimento do disposto nesta Política, ou nas normas e procedimentos sobre Segurança da Informação e Comunicações e Segurança Cibernética, acarreta a aplicação das penalidades previstas nas normas internas do Banco da Amazônia.