ICBC do Brasil Banco Múltiplo S.A.

Política de Segurança da Informação e Segurança Cibernética - Resumida

INFORMAÇÃO PÚBLICA
As informações contidas neste documento foram classificadas pelo proprietário como sendo PÚBLICAS.

1. INTRODUÇÃO

O objetivo da política de cibersegurança é demonstrar o compromisso da nossa organização em proteger nossos ativos digitais. Esta política se aplica a todos os funcionários, terceiros, clientes e parceiros que tenham acesso à nossa infraestrutura.

2. FUNÇÕES E RESPONSABILIDADES

Todos os funcionários, terceiros, clientes e parceiros compartilham a responsabilidade de garantir a segurança dos nossos ativos digitais. Embora a nossa equipe de Cibersegurança e TI lidere a manutenção da segurança, todos têm um papel a desempenhar na proteção da nossa organização.

3. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

- **Autenticidade:** garantir que a informação veio da fonte anunciada, de modo que seja possível confirmar sua autoria e originalidade.

- **Confidencialidade:** garantir que o acesso à informação seja obtido somente por pessoas autorizadas.

- **Integridade:** garantir a exatidão e integridade das informações e seus métodos de processamento, a fim de protegê-las contra alterações impróprias, intencionais ou acidentais, durante a custódia ou transmissão.

- **Disponibilidade:** garantir que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

4. CONTROLES DE SEGURANÇA

Uma combinação de medidas técnicas e administrativas é implementada para proteger nossos ativos digitais. Essas medidas incluem, mas não se limitam a controles de acesso, criptografia, firewalls, detecção de intrusão e software antivírus.

5. CONTROLE DE ACESSO

Para assegurar um controle de acesso eficiente, adotamos autenticação robusta, autorização baseada em políticas e segregação de funções. Seguimos uma política de senha segura, atribuindo perfis de acesso conforme as responsabilidades e monitorando os registros de acesso. Seguindo essas práticas estamos protegendo os dados e recursos do sistema contra uso indevido e acesso não autorizado.

6. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações devem ser categorizadas com base em sua confidencialidade e proteções necessárias, usando os seguintes níveis: Restrito, Confidencial, Interno e Público. Ao fazer isso, as necessidades relacionadas aos negócios, o compartilhamento ou restrição de acesso e as consequências do uso inadequado das informações devem ser levados em consideração.

7. RESPOSTA A INCIDENTES

No caso de um incidente de cibersegurança, seguiremos nosso plano de resposta a incidentes para conter e mitigar a situação. Todos os funcionários devem reportar qualquer suspeita ou incidente de cibersegurança à nossa equipe de cibersegurança imediatamente.

8. TREINAMENTO E CONSCIENTIZAÇÃO DOS FUNCIONÁRIOS

Forneceremos treinamento regularmente a todos os funcionários para aumentar a conscientização sobre riscos de cibersegurança e melhores práticas. Também realizaremos campanhas contínuas de conscientização sobre segurança para lembrar a todas suas responsabilidades na proteção dos nossos ativos digitais.

9. GERENCIAMENTO DE INCIDENTES POR PROVEDORES TERCEIRIZADOS

Os contratos do ICBC Brasil com prestadores de serviços são formalizados, avaliados (quanto à criticidade dos riscos), monitorados e revisados. Quando qualquer prestador terceirizado contratado com o ICBC Brasil tiver acesso a informações e sistemas de informação do Banco, o contrato ou contrato de serviço deverá especificar a responsabilidade de segurança do prestador e os requisitos de segurança que devem ser seguidos.

10. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS EM NUVEM

A segurança de dados é uma preocupação importante para qualquer empresa que utilize serviços em nuvem. Quando se trata de provedores de terceiros, é importante garantir que eles estejam em conformidade com as leis e regulamentações aplicáveis e que sigam práticas de segurança rigorosas. Isso pode incluir o uso de criptografia para proteger dados confidenciais, o uso de firewalls para impedir o acesso não autorizado e a implementação de políticas que monitoram e marcam atividades suspeitas. Além disso, as empresas devem ter um plano de contingência em caso de violação de dados e garantir que seus funcionários estejam treinados em práticas seguras de uso de dados.

11. CONFORMIDADE E REGULAMENTAÇÕES

Adotaremos todas as leis e regulamentações pertinentes relacionadas à cibersegurança. Nossa equipe de cibersegurança se manterá informada sobre as últimas leis e regulamentações, garantindo que nossa organização permaneça em conformidade, incluindo a Res. BACEN 4893.

12. REVISÃO E ATUALIZAÇÕES DA POLÍTICA

Analisaremos e atualizaremos regularmente esta política de cibersegurança para garantir sua relevância e eficácia continuamente. Todos os funcionários, terceiros, clientes e parceiros serão notificados sobre quaisquer atualizações de política.

A efetividade das políticas de Segurança da Informação é verificada por meio de avaliações periódicas de Auditoria Interna.

Aprovado pelo Conselho de Administração em 20/03/2023