SANY
BANCO

Política de Segurança da Informação e Cibernética

Banco Sany Brasil S/A

JANEIRO, 2026

ÍNDICE

1. INTRODUÇÃO

Os objetivos da Política de Segurança da Informação e Cibernética são:

- Compreender a necessidade de sigilo sob quaisquer informações que se possua acesso para execução de seu trabalho, desta forma mantendo os dados/informações e estratégias do Banco somente dentro do grupo organizacional, não fornecendo a terceiros, salvo com existência de autorização expressa da Presidência do Banco.
- Delinear a forma de uso aceitável dos equipamentos, softwares e sistemas de informação do BANCO SANY. As orientações e regras aqui contidas são estabelecidas para prover meios de proteção aos Funcionários, clientes, parceiros, especialistas, Funcionários contratados em regime temporário, incluindo pessoal integrante de empresas contratadas, contra ameaças, incluindo ataques de vírus, comprometimento da rede e dos serviços e assim como contra sanções legais.
- Orientar sobre o uso, armazenagem e destruição de documentos contendo informações confidenciais, sejam relativas aos clientes, sejam relativas aos negócios do Banco, bem como os riscos associados ao uso e destruição inadequada deles.

1.1 Atribuições e Responsabilidades

Diretoria

- Deliberar sobre normas internas de segurança da informação;
- Respaldar financeiramente projetos de melhoria da segurança da informação e cibernética do **BANCO SANY**.

Gerente de TI

- Analisar casos de violação da segurança da informação, tomando providências imediatas;
- Garantir a divulgação da política de segurança da informação, bem como das normas e procedimentos vinculados a esta política;

- Realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação e dos demais ambientes em que circulam as informações do **BANCO SANY**;
- Analisar e mitigar os riscos relacionados à segurança da informação;
- Requisitar informações das demais áreas, com o intuito de verificar o cumprimento da Política e das Normas da segurança da informação;
- Obter as informações necessárias para a elaboração do Relatório de Impacto à Proteção de Dados Pessoais;
- Comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular dos dados pessoais a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante a esses dados.

1.2 Responsabilidades Gerais

- Todas as informações trocadas ou armazenadas no **BANCO SANY**, independentemente de conteúdo, são de propriedade única e exclusiva do Banco. Os usuários devem utilizar os recursos disponibilizados pelo Banco apenas para a condução dos negócios do Banco;
- Compete a todos os Colaboradores o cumprimento das diretrizes constantes desta Política e das demais diretrizes de Segurança da Informação e Cibernética;
- Todo colaborador deve aderir, formalmente, ao Contrato/Termo de Segurança;
- Devem informar imediatamente, à Área de Gestão de Riscos todas as violações às políticas de segurança da informação, incidentes, violações de acessos ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento.

2. PRINCIPAIS CARACTERÍSTICAS

A Estrutura normativa da Segurança da Informação do **BANCO SANY** é composta por um conjunto de documentos com níveis hierárquicos distintos, relacionados a seguir:

- Política de Segurança da Informação: define estrutura, diretrizes e as obrigações referentes a segurança da informação;

- Normas de Segurança da Informação: estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada;

- Procedimentos de Segurança da Informação: instrumentalizam o disposto nas Normas e na Política, permitindo a direta aplicação nas atividades do Banco.

3. SEGURANÇA CIBERNÉTICA

O **BANCO SANY** tem como visão garantir a proteção, a manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações da sua propriedade, além de prevenir, detectar e reduzir a vulnerabilidade a incidentes que tenha relação com o ambiente cibernético, definindo as regras que representam, a nível estratégico, os princípios do **BANCO SANY** focados no objetivo de segurança da informação.

3.1 Princípio da Segurança Cibernética

Acreditamos que os ativos de informação são os bens mais relevantes no mercado financeiro, com isso, é nosso dever tratá-los com responsabilidade. O fundamento do **BANCO SANY** está no princípio direto a segurança da informação, cujos objetivos constituem a preservação da propriedade da informação, com sua confidencialidade, integridade e disponibilidade, autorizando o uso e compartilhamento de forma controlada, com o monitoramento e tratamento de incidentes oriundos de ataques cibernéticos.

- **Confidencialidade:** garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas.
- **Integridade:** garantir que as informações sejam integras, sem modificações indevidas – acidentais ou propositais.
- **Disponibilidade:** garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

3.1.1 Informações Confidenciais

O acesso às informações confidenciais, sendo esses também dados pessoais, coletados e arquivados pelo **BANCO SANY**, deve ser restrito aos profissionais autorizados ao uso direto dessas informações, é necessário a prestação de seus

serviços, sendo limitado o uso para outras atividades, deve ser respeitado ainda, o disposto na norma de classificação da informação.

As informações confidenciais devem ser reveladas nas seguintes hipóteses:

- Quando for obrigado a revelá-las através de formalidade legal, ato de autoridade, ordem ou mandado judicial;
- Aos órgãos de proteção ao crédito e prestadores de serviços autorizados pelo **BANCO SANY**;
- Aos órgãos reguladores do mercado financeiro;
- Para outras instituições financeiras, desde que dentro dos parâmetros legais.

3.2 Estrutura de Gerenciamento de Segurança Cibernética

O objetivo do gerenciamento de controles de segurança é assegurar que os procedimentos operacionais sejam elaborados, implantados ou modificados de acordo com os objetivos estabelecidos nesta política.

3.2.1 Gestão de Acesso às Informações

Os acessos as informações são controlados, monitorados, sendo restrito à menor permissão e privilégios possíveis, revisados periodicamente, e cancelados pontualmente ao término do contrato de trabalho do colaborador ou prestador de serviço.

Os equipamentos e instalações de processamento de informações são mantidos em áreas seguras, com controle incluindo proteção contra ameaças físicas e ambientais.

Os colaboradores são conscientizados através de treinamentos via intranet sobre os conceitos de segurança da informação.

3.2.2 Autenticação

O acesso as informações e aos ambientes tecnológicos do **BANCO SANY** deve ser permitido apenas às pessoas autorizadas, levando em consideração a segregação de funções.

O controle de acesso aos sistemas deve ser formalizado com os seguintes controles:

- A utilização de login (credencial de acesso) individual, monitorado e passiveis de bloqueios e restrições;
- A exclusão de autorizações dadas a usuários afastados ou desligados do Banco ou que ainda tenha mudado de função;
- A revisão periódica das autorizações concedidas.

3.2.3 Prevenção a Vazamento de Informações

Utilização de controle para prevenção de perda de dados, responsável por garantir que dados confidenciais não sejam perdidos, roubados, mal utilizados ou vazados na web por usuários não autorizados.

3.2.4 Varredura de Vulnerabilidades

As varreduras das redes internas e externas devem ser checadas periodicamente. As vulnerabilidades identificadas devem ser tratadas e priorizadas de acordo com seu nível de reparo.

3.2.5 Redução da Vulnerabilidade

Os processos utilizados para a análise de vulnerabilidades são:

- Atualização do inventário de ativos de TI, com a atribuição de critérios de relevância de cada ativo e de seus dados para os negócios e operações;
- Identificação das vulnerabilidades ou ameaças potenciais para cada ativo; e
- Mitigação ou eliminação das vulnerabilidades mais graves dos ativos mais importantes.

Para a análise de vulnerabilidades, o **BANCO SANY** dispõe de processos e ferramentas especializadas e reconhecidas nos mercados nacional e internacional para:

- Registrar, monitorar e analisar as operações de acesso, a fim de proteger seus registros (logs) e assegurar a devida rastreabilidade;
- Gestão dos acessos às informações por meio de segregação de funções assegurando o controle de acessos de acordo com cada função, para o correto tratamento e processamentos dos dados; e
- Realizar periodicamente testes e varreduras para detecção de vulnerabilidades em sistemas.

3.2.6 Teste de Intrusão e Scan de Vulnerabilidades

- Anualmente são realizados testes de intrusão e scan de vulnerabilidades para a prevenção de vazamento de informações, checagem de proteção contra softwares maliciosos e detecção de aderência de patches de software;
- O escopo é interno e externo, abrangendo sistemas internos de Tecnologia e de Negócios. Farão parte dos testes os firewalls de borda de Internet, testando conexões e IPs externos da rede;
- Apenas empresas especializadas serão contratadas para a execução do trabalho.

3.2.7 Controle Contra Software Malicioso

Computadores e servidores que estejam conectados à rede corporativa ou façam uso das informações do **BANCO SANY**, devem ser protegidos com uma solução anti-malware determinada pela área de segurança da informação.

3.2.8 Criptografia

Toda resolução de criptografia utilizada no **BANCO SANY** deve seguir as regras de segurança da informação e os padrões de segurança dos órgãos reguladores.

3.2.9 Rastreabilidade

Toda informação sensível deve ser identificada, justificado seu uso e receber esta classificação, sendo que as informações classificadas como “sensíveis” devem receber níveis adicionais de proteção e rastreabilidade.

Todos os sistemas que tratam informação classificada como sensível mantém log de acessos de leitura, escrita e alteração são registrados nos concentradores de log com a trilha de auditoria para o tratamento da informação sensível.

São utilizados recursos tecnológicos como criptografia, concentrador de registros (logs) de rede com análise proativa e procedimentos de resposta a incidentes cibernéticos. Estes recursos são continuamente geridos por pessoal específico e especializado.

Processos e procedimentos são adotados pelas áreas de Tecnologia da Informação, Sistemas, e Riscos, a fim de garantir a manutenção da segurança cibernética e manter os riscos cibernéticos sob nível adequado de controle.

Sistemas de autenticação devem ser automatizados para monitorar os seguintes eventos:

- Autenticação de usuários (tentativas válidas e inválidas);
- Acesso a informações;
- Ações executadas pelos usuários, incluindo criação ou remoção de objetos do sistema.

3.2.10 Desenvolvimento Seguro

O **BANCO SANY** utiliza de um conjunto de princípios para desenvolver sistemas de forma segura, garantindo que a segurança cibernética seja projetada e implementada no ciclo de vida de desenvolvimento de sistemas.

3.2.11 Backup

A execução de backups é realizada, de forma periódica nos ativos de informação do **BANCO SANY** de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

3.3 Principais Recomendações de Segurança aos Clientes e Usuários

3.3.1 Autenticação e Senha

- O cliente é responsável pelos atos executados com seu login, que é único e sua senha de uso pessoal e intransferível;
- É importante manter a sua confidencialidade, memorize e não registre a senha em lugar algum. Ou seja, não compartilhar com ninguém e nem anotar em nenhum papel;
- Realizar a alteração de sua senha sempre que existir qualquer suspeita do comprometimento dela;
- Cadastrar senhas de qualidade e de difícil adivinhação;
- Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado / logado com a sua identificação;
- Bloquear sempre o equipamento ao se ausentar do ambiente.

3.4 Tipos de abordagens maliciosas

3.4.1 Engenharia Social

A engenharia social refere-se à técnica pela qual uma pessoa procura persuadir outra, muita das vezes abusando da ingenuidade ou confiança do usuário, com o objetivo de ludibriar, aplicar golpes ou obter informações sigilosas.

3.4.2 *Phishing*

Técnica utilizada por criminosos para enganar os usuários, através de envio de e-mails maliciosos, para obtenção de informações pessoais como senhas, cartão de crédito, CPF, número de contas bancárias etc. As abordagens podem ocorrer das seguintes maneiras:

- Para atrair atenção do usuário, no objetivo de obter alguma vantagem financeira;
- Quando tentam se passar por instituições como: Bancos, Lojas de comércio eletrônico, ou sites;
- Tentam induzir usuários a preencher formulários com os seus dados pessoais ou financeiros, ou até a instalação de softwares maliciosos com o objetivo de coletar informações sensíveis.

3.4.3 *Spam*

E-mails não solicitados, os quais geralmente são enviados para muitas pessoas, possuindo tipicamente conteúdo com fins publicitários. Além disso, os Spams estão diretamente associados a ataques de segurança, tornando-se um dos principais propagadores de códigos maliciosos, venda ilegal de produtos e disseminação de golpes.

3.4.4 Ligação Falsa

São técnicas utilizadas pelos fraudadores para conseguir informações como dados pessoais, senhas, token, código de identificação do aparelho celular ou qualquer tipo de informação para a prática de fraude.

3.5 Processamento, Armazenamento de dados e Computação em Nuvem

Para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, o **BANCO SANY** assegura-se de um procedimento efetivo aderente às regras previstas na regulamentação em vigor.

O Banco realizará o tratamento de dados e informações em meio digital por meio de soluções desenvolvidas ou adquiridas, considerando os princípios de segurança da informação: disponibilidade, integridade, confidencialidade, autenticidade, irretratabilidade, privilégio mínimo, necessidade de conhecer, proteção de dados pessoais e proteção da privacidade.