Banco Mizuho do Brasil S.A.
Política de Segurança Cibernética

Com o objetivo de estabelecer o procedimento fundamental para a realização da proteção e utilização dos recursos de informação do Banco Mizuho do Brasil S.A. ("Banco"), em atendimento à Resolução CMN 4.893/21 e alinhado às políticas globais do Grupo, o Banco torna público e descreve, por meio deste documento, o resumo dos Procedimentos de Segurança Cibernética e os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

1. Ativos de Informação

Cada funcionário, estagiário e estatutário deve garantir a confidencialidade, integridade e disponibilidade dos Ativos de Informação de acordo com sua ordem de importância, que serão classificadas como:

- Informação Crítica: requer gerenciamento severo, uma vez que pode causar impacto crítico ao objeto da informação (clientes, administração e operação do Banco) em caso de vazamento;
- Informação Importante: requer um gerenciamento robusto, uma vez que pode causar impacto significante ao objeto da informação em caso de vazamento ou uso indevido;
- Informação Regular: impacto limitado, porém é exigido gerenciamento apropriado;
- Público: informações preparadas pelo Banco, que são divulgadas externamente.

2. Medidas de Recursos Humanos relacionadas à Segurança da Informação

2.1. Obrigação de Não-Divulgação e Confidencialidade

Todo funcionário, estagiário e estatutário terá a obrigação de não-divulgação em relação as informações adquiridas no curso de suas funções.

2.2. Esclarecimento dos Papéis, Funções e Responsabilidades de Funcionários, Estagiários, Estatutários e Eventuais Temporários ou Prestadores de Serviços Terceirizados

O Banco deverá ter determinado claramente as funções e responsabilidades dos funcionários, estagiários e estatutários, bem como estabelecer disposições em contrato para eventuais temporários ou prestadores de serviços terceirizados em relação à Segurança Cibernética.

2.3. Formação e Capacitação

O Banco deverá realizar programas de formação e capacitação, visando a disseminação do conhecimento específico certificando-se de que todos os funcionários, estagiários e estatutários estejam cientes das leis, regulamentos aplicáveis, normas e regulamentos internos relacionados à Segurança Cibernética.

2.4. Confirmação de Conformidade

O Banco deverá, anualmente, realizar inspeções, auditorias, confirmações e monitoramento da situação de conformidade dos funcionários, estagiários e estatutários em relação as normas e regulamentos internos do Banco, incluindo estes procedimentos.

2.5. Disciplina

O Banco deverá responder de forma rigorosa e justa a qualquer violação de aplicação das leis e regulamentos, e das normas e regulamentos internos do Banco, incluindo este Procedimento, relacionados à Segurança Cibernética.

3. Mecanismos

O Banco deverá estabelecer mecanismos de acompanhamento e de controle com vistas a assegurar a implementação e a efetividade da política de segurança cibernética, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

4. Controles

O Banco deverá estabelecer as funções de controle e auditoria interna necessárias e realizar anualmente auditorias com o intuito de verificar a conformidade de cada Departamento com a aplicação das leis e regulamentos relacionados à Segurança Cibernética.

5. CIRT (*Computer Incident Response Team*)

O Banco deverá preparar uma estrutura organizacional que permita medidas de respostas rápidas e apropriadas a serem tomadas caso incidentes cibernéticos ocorram no Banco.

6. Planos de Continuidade de Negócios

O Banco deverá preparar planos de continuidade de negócios apropriados para minimizar a extensão do dano para os Ativos de Informação e restaurar de forma rápida e eficiente as operações de negócios, em caso de desastre natural, acidente, interrupção ou outra calamidade.

7. Disseminação da Cultura

A Diretoria deverá garantir os meios necessários para o cumprimento deste Procedimento, por meio do:

- Gerenciamento adequado do Risco da Segurança Cibernética;
- Aplicação eficaz e contínua deste Procedimento;
- Comunicação efetiva e treinamento deste Procedimento para todos os funcionários, estagiários e estatutários;
- Fomento de uma cultura de Segurança Cibernética no Banco;
- Reporte sempre que identificados indícios de violações, vazamento de informação ou problemas relacionados à Segurança Cibernética.

8. Gerenciamento das Operações Terceirizadas

O Banco deverá realizar gerenciamento apropriado da terceirização de suas operações com o intuito de impedir vazamentos dos Ativos de Informação ou incidentes de Segurança Cibernética, quando o Banco terceirizar a totalidade ou partes de uma operação que envolva a utilização dos Ativos de Informação.

O Banco deverá avaliar para cada serviço contratado (ou a ser contratado) de terceiros, a criticidade do serviço e a sensibilidade dos dados e informações a serem processadas, arquivadas e gerenciadas por tal fornecedor de serviços.

São definidos como serviços críticos de acordo com o regulador:

- Processamento de Dados;
- Armazenamento de Dados;
- Serviços de Nuvem.

Banco Mizuho do Brasil S.A.