Política de Segurança da Informação e Segurança Cibernética

Classificação da Informação	INTERNO

Responsável pelo Documento	Área
Elaboração	Segurança da Informação e Segurança Cibernética
Revisão	Risco Operacional & Controles Internos Diretoria de Controles Internos, RH, Compliance & PLDFT, Segurança da Informação e Segurança Cibernética
Aprovação	Diretoria Executiva

Registro de Alterações:

Versão	Item Modificado	Data de Aprovação
01	Versão Inicial	06/08/2018
02	• Inclusão do termo Segurança Cibernética	03/12/2018
03	• Adequação de Modelo	02/05/2019
04	• Inclusão de Normas	13/09/2019
05	• Revogar a versão 04 • Alteração: novo formato, alteração geral de conteúdo e Inclusão do item 10 DA PRIVACIDADE DOS DADOS PESSOAIS	28/12/2020
06	• Revisão integral, incluindo atualizações normativas e nova razão social.	19/11/2021
07	• Revisão periódica	24/01/2023
08	• Revisão Geral Conteúdo e adesão aos aspectos do Banco de Investimentos (BI)	27/03/2023

ÍNDICE

1 OBJETIVO

Este documento tem por finalidade estabelecer as diretrizes da Política de Segurança da Informação e Segurança Cibernética do Banco Master S.A., da Master S.A. Corretora de Câmbio, Títulos e Valores Mobiliários, do Banco Master de Investimento S.A. e das demais sociedades coligadas, controladas, controladoras e sob controle comum que integrem o grupo econômico ("Grupo Master").

Estas diretrizes servem como base para as normas, padrões e procedimentos que regulamentam os processos aqui definidos como importantes para uma boa prática da gestão da Segurança da Informação.

2 ABRANGÊNCIA

Este procedimento abrange todos os colaboradores (empregados, estagiários, menor aprendiz, fornecedores, parceiros de negócio, prestadores de serviços e contratados), todos os serviços e recursos de TI e telecomunicações em tráfego de dados e armazenamento em uso, seja por dispositivos próprios ou contratados.

3 VIGÊNCIA

Esta Política entra em vigor na data da sua aprovação e revoga toda e qualquer das versões previamente publicadas e aprovadas.

A atualização da Política poderá ocorrer a qualquer tempo no caso de alterações na regulamentação vigente ou no caso de mudanças relevantes nos processos internos a ela relacionados.

4 APROVAÇÃO DE EXCEÇÕES

Qualquer exceção das Normas e Procedimentos contidos neste documento, somente será realizado quando aprovado pelo Comitê de Segurança da Informação. Uma cópia da autorização da exceção deverá ser encaminhada ao responsável pela gerência de Segurança da Informação que devem ser mantidas junto aos dossiês das operações e registradas nos sistemas para eventuais necessidades de verificação por auditoria, supervisão ou testes de controles internos.

5 ASPECTOS REGULATÓRIOS

Órgão Regulador	Número do Requerimento	Título/Resumo
BACEN	Resolução CMN nº 4.893, de 26 de fevereiro de 2021	Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.
BACEN	Instrução Normativa BCB nº 134, de 22 de julho de 2021	Divulga a versão 3.0 do Manual de Segurança do Open Banking.
Presidência da República	Lei nº 13.709, de 14 de agosto de 2018 - LGPD - **Lei Geral de Proteção de Dados Pessoais** e suas alterações pela Lei nº 13.853, de 8 de julho de 2019	Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
Presidência da República	Lei nº 12.965, de 23 de abril de 2014	Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.
ABNT/ISO	NBR/ISO 27001	Esta Norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de

		riscos de segurança da informação voltados para as necessidades da organização.
Comissão de Valores Mobiliários	Resolução CVM nº 29, de 11 de maio de 2021	Dispõe sobre as regras para constituição e funcionamento de ambiente regulatório experimental (sandbox regulatório) e revoga a Instrução CVM nº 626, de 15 de maio de 2020.
Comissão de Valores Mobiliários	Resolução CVM nº 35, de 26 de maio de 2021	Estabelece normas e procedimentos a serem observados na intermediação de operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários e **revoga** a Deliberação CVM nº 105, de 22 de janeiro de 1991, e **as Instruções** CVM nº 51, de 9 de junho de 1986, CVM nº 333, de 6 de abril de 2000, **CVM nº 505, de 27 de setembro de 2011**, Instrução CVM nº 526, de 21 de setembro de 2012; Instrução CVM nº 581, de 29 de setembro de 2016; Instrução CVM nº 612, de 21 de agosto de 2019; e Instrução CVM nº 618, de 28 de janeiro de 2020.

6 NORMATIVOS INTERNOS APLICÁVEIS

Política, Manual de Procedimento ou Norma	Título
Norma	Norma de Contratação de Prestadores de Serviço de TI e SI: Recursos em Nuvem
Norma	Norma para o Plano de Ação e de Resposta a Incidentes
Procedimento	Plano de Ação e de Respostas a Incidentes
Norma	Norma da Classificação da Informação
Norma	Norma de Solicitação e Controle de Acesso

7 DISPOSIÇÕES GERAIS

7.1 Definições

1. A **Informação** é um ativo estratégico e de alto valor para o Grupo Master, de sua propriedade ou sob sua responsabilidade e deve ser protegida, em conformidade com a legislação vigente, com os valores éticos e com as melhores práticas da segurança da informação;

2. A **Segurança da Informação** constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade, disponibilidade e privacidade, permitindo o uso e o compartilhamento da informação de forma controlada, independentemente do meio de armazenamento, processamento ou transmissão que seja utilizado;

3. O termo **Segurança Cibernética (Cyber Security)** é utilizado para designar o conjunto de meios e tecnologias empregadas na defesa dos sistemas de informação, infraestrutura, redes de computadores e/ou dispositivos pessoais, com o objetivo de prevenir danos, roubo, intrusão, alterações ou destruição da informação ocasionados por ataques cibernéticos e está integralmente inserido na presente Política;

4. **Incidente de Segurança** é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade, tais como invasões de computador, ataques de negação de serviços, furto de informação por pessoal interno e ou terceiros, vazamento de dados, atividades em rede não autorizadas ou ilegais;

5. **Resposta a Incidentes** é o processo previamente definido que descreve como o Grupo Master deverá lidar com um incidente de segurança;

6. **Equipe de Resposta a Incidentes** é o grupo responsável por analisar e responder, com rapidez e precisão, os incidentes de segurança do Grupo Master. É previamente definido e imediatamente acionado para efetuar as análises necessárias, pois o tempo de resposta é fundamental para minimizar as consequências e proteger as informações críticas;

7. **Sala de Resposta a Incidentes** é o local físico ou virtual, onde a Equipe de Resposta a Incidentes se reunirá no caso da ocorrência de um Incidente de Segurança. Contém os recursos necessários para a Equipe atuar com eficiência e eficácia.

7.2 Objetivos

1. Proteger o valor e a reputação da empresa;

2. Garantir a confidencialidade, integridade, disponibilidade e privacidade das informações do Grupo Master, e de informações de terceiros por ela custodiadas, contra acessos indevidos e modificações não autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, quando necessário;

3. Identificar violações de Segurança da Informação, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes;

4. Garantir a continuidade dos negócios do Grupo Master, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;

5. Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da empresa;

6. Conscientizar, educar e treinar os usuários na política, normas e procedimentos de Segurança da Informação para que sejam aplicadas às suas atividades diárias;

7. Estabelecer e melhorar continuamente um Processo de Gestão de Riscos de Segurança da Informação e Segurança Cibernética.

8 PAPÉIS E RESPONSABILIDADES

8.1 Da Alta Direção

A Alta Direção deve prover comprometimento e apoio à aderência da Política de Segurança da Informação e Segurança Cibernética de acordo com os objetivos e estratégias do negócio do Grupo Master.

8.2 Gerência de Segurança da Informação e Comitê de Segurança da Informação

A Gerência de Segurança da Informação e o Comitê de Segurança da Informação são responsáveis por custodiar, manter e divulgar esta Política, bem como assegurar que todos os assuntos relacionados com a segurança da informação sejam tratados de uma maneira consistente e efetiva.

A Gerência de Segurança de Informação é responsável, também, por incrementar a consciência de segurança de informação a todos integrantes mencionados no tópico “Abrangência” desta Política.

8.3 Gestores

Todo gestor é responsável por assegurar o cumprimento da Política pelos funcionários de sua área, atuando de forma coordenada com a Gerência de Segurança da Informação, bem como assegurar que os contratos e serviços sob sua responsabilidade estejam aderentes à esta Política e demais Normais e Procedimentos de Segurança.

8.4 Colaboradores

Todo empregado, estagiário, menor aprendiz, fornecedor, parceiro de negócio ou prestador de serviços é responsável por proteger as informações da empresa e relatar qualquer situação que represente desvio ou violação da segurança destas, bem como atender as recomendações pertinentes, constantes nas normas e procedimentos de segurança da empresa.

9 ADESÃO

A adesão à presente Política implica estrita observância das regras contidas nela e na legislação vigente, sob pena de aplicação de sanções disciplinares. A adesão dos Colaboradores a esta Política será formalmente confirmada por meio da assinatura de "Termo de Adesão a Política de Segurança da Informação e Segurança Cibernética".

A cada alteração desta Política, serão circuladas mensagens eletrônicas aos Colaboradores, com resumo sobre a alteração realizada e, sempre que as alterações forem consideradas pelo Comitê de Segurança da Informação como relevantes e/ou importarem obrigações adicionais aos Colaboradores, os Colaboradores deverão reiterar a sua adesão às normas de Segurança da Informação por meio da assinatura de "Termo de Adesão às Alterações da Política de Segurança da Informação e Segurança Cibernética", conforme modelo constante do Anexo II da presente Política.

10 SANÇÕES APLICÁVEIS A NÃO CONFORMIDADE

O Comitê de Segurança da Informação do Grupo Master deve garantir que medidas corretivas sejam tomadas quando falhas de conformidade forem identificadas. Qualquer violação ou suspeita de violação a esta Política, bem como às Normas, Procedimentos e Planos que a compõem, identificada pelos Colaboradores deve ser levada ao conhecimento da Gerência de Segurança da Informação, que deverá reportar o assunto para a análise do Comitê de Segurança da Informação.

O Comitê de Segurança da Informação deve proferir decisão em até 30 (trinta) dias sobre a aplicação ou não de sanção disciplinar à eventual violação a esta Política.

11 DA PRIVACIDADE DOS DADOS PESSOAIS

O Grupo Master é responsável por garantir que os dados pessoais não sejam perdidos, roubados, utilizados indevidamente ou vazados por usuários não autorizados, desta forma utiliza controles para prevenção de perda de dados, visando mitigar os riscos usuais, com o estabelecimento de mecanismos de governança, a avaliação e melhoria contínua de todos os aspectos específicos de privacidade e proteção de dados pessoais.

As diretrizes estabelecidas neste documento, e todos aqueles que ficam a elas obrigados, deverão observar e cumprir a legislação aplicável à Proteção de Dados Pessoais, em especial a Lei nº 13.709/2018 e suas alterações posteriores ("Lei Geral de Proteção de Dados" ou "LGPD"), bem como as normas internas de Proteção de Dados Pessoais do Grupo Master.

Quaisquer questões relacionadas à Proteção de Dados Pessoais no âmbito do Grupo Master deverão ser encaminhadas para: privacidade@bancomaster.com.br.

12 DOCUMENTAÇÃO COMPLEMENTAR

A presente Política de Segurança da Informação e Segurança Cibernética é complementada através das normas, procedimentos e planos de segurança publicados na Intranet.