GRUPO MERCANTIL

Política de Segurança da Informação

Vigência a partir de

28/01/2025

Validade

28/01/2027

Versão

02

Divulgação EXTERNA

Sumário

1. APRESENTAÇÃO

A presente Política Institucional é aplicável a todos que estão indicados no item "Abrangência" deste documento.

Esta Política visa evitar e mitigar que dados e informações corporativas do Banco Mercantil sejam destruídas, modificadas, divulgadas, acessadas de forma indevida, seja de forma acidental ou intencional.

Estabelecer processos para preservar a integridade, confidencialidade e disponibilidade das informações e dados de propriedade do Banco Mercantil.

2. BASE LEGAL

Tipo	Número/Ano	Objetivo
Lei Geral de Proteção de Dados - LGPD	13.709/2018	Tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
Lei Marco Civil da Internet	12.965/2014	Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil
Oficio Circular CVM/SMI	1/2024/CVM/SMI	O presente Ofício-Circular tem o objetivo manifestar o entendimento da Superintendência de Relações com o Mercado e Intermediários da CVM quanto ao procedimento a ser observado pelos intermediários no monitoramento e na comunicação à CVM de indícios de descumprimento à legislação que incumbe a esta autarquia fiscalizar, nos termos dos incisos IV e IX do art. 33 da Resolução CVM nº 35, de 26 de maio de 2021, e da Resolução CVM nº 50, de 31 de agosto de 2021.

3. ABRANGÊNCIA

Esta Política se aplica ao Banco Mercantil e às empresas do Grupo Mercantil. A ciência e o cumprimento das diretrizes e regras aqui estabelecidas são obrigatórios a todos os seus colaboradores e terceiros.

4. GLOSSÁRIO DE TERMOS E SIGLAS

- Integridade: Garantir que os dados, informações mantenham seu estado original, seja em repouso ou em trânsito, para que não ocorra quaisquer tipos de alterações;
- Confidencialidade: Garantir que os dados, informações sejam acessados somente pelas pessoas que realmente deva ter acesso;
- Disponibilidade: Garantir que os dados, informações estejam disponíveis a qualquer momento, sem quaisquer interrupções ou inacessibilidade.

5. CUMPRIMENTO, SANÇÕES E PENALIDADES

Todos os funcionários, parceiros de negócios e terceiros prestadores de serviços devem estar cientes da sua responsabilidade pessoal no cumprimento rigoroso da conduta considerada adequada, conforme prescrito nos Manuais de Procedimentos de Segurança da Informação.

O Banco se reserva o direito de averiguar, tempestivamente, se os funcionários cumprem todos os direitos e deveres a eles atribuídos, em decorrência do uso dos ativos de Tecnologia da Informação e demais recursos de propriedade das empresas do Grupo Mercantil.

Em caso de descumprimento da Política de Segurança da Informação, o Mercantil poderá realizar ações disciplinares, rompimentos contratuais ou outras medidas consideradas apropriadas, de acordo com a gravidade do ato. Periodicamente, são efetuadas avaliações sobre o nível de aderência às normas e aos procedimentos relativos à Política de Segurança da Informação e suas diretrizes.

Aos parceiros e terceiros prestadores de serviços serão encaminhadas cópias digitais da Política de Segurança da Informação, a fim de que estas sejam repassadas aos colaboradores que prestam serviços ao Grupo Mercantil.

Aos funcionários, parceiros de negócios e terceiros prestadores de serviços é vedada a faculdade de alegar desconhecimento da Política de Segurança da Informação do Grupo Mercantil.

Cada área ou unidade organizacional do Grupo Mercantil deverá elaborar e fazer cumprir as normas de Segurança da Informação aplicáveis aos seus processos de negócios, em conformidade com os ditames definidos nesta Política.

6. PROPRIEDADE DE RECURSO

I. São considerados propriedade das empresas do Grupo Mercantil:

a) Todo equipamento, peça, periférico ou meio adquirido com recursos das empresas Mercantil;

b) Todo programa e/ou sistema adquirido ou produzido com recursos das empresas Mercantil;

c) Todo esquema, diagrama, dispositivo, programa de computador, sistema ou aplicativo desenvolvido, aperfeiçoado ou executado por empregado ou prestador de serviços de qualquer empresa Mercantil, independentemente do meio de apresentação e/ou armazenagem, para o qual tenha sido utilizado pelo menos um dos seguintes elementos:

- Recursos financeiros das empresas Mercantil ou a elas confiados por terceiros;
- Recursos materiais de propriedade das empresas Mercantil ou sobre os quais elas tenham responsabilidade;
- Recursos humanos remunerados pelas empresas Mercantil durante seu período de atividades vinculadas a tarefas e responsabilidades imputadas no seu exercício profissional, ou por elas contratados como prestadores de serviços.

d) Dados e informações registrados, armazenados e recuperáveis por quaisquer meios viabilizados pelo emprego dos três recursos enumerados na alínea "c" deste parágrafo.

II. São considerados propriedade de terceiros:

a) Todo equipamento, peça ou dispositivo físico que o terceiro possa dispor quanto ao uso, à posse e à titularidade;

b) Todo programa e/ou sistema que o terceiro possa dispor quanto ao uso, à posse e à titularidade;

c) Toda informação ou dado registrado, mantido e/ou recuperado por terceiro.

As informações criadas, enviadas, recebidas e armazenadas nos ativos de Tecnologia da Informação que sejam consideradas propriedade do Grupo Mercantil são passíveis de monitoramento e auditagem, generalizada ou específica, não caracterizando invasão de privacidade.

As informações originadas nas condições deste documento não são privativas e são de interesse único e exclusivo das empresas do Grupo Mercantil, que pode inspecionar quaisquer arquivos armazenados nos ativos de Tecnologia, mesmo que eles não estejam em suas dependências.

7. PRINCÍPIOS

Os princípios primordiais da Política de Segurança do Grupo Mercantil constituem-se em:

a) Proteger as informações e os sistemas contra acesso, modificação, destruição ou divulgação não autorizados, certificando-se que as ferramentas e tecnologias adotadas pela empresa estão a serviço de tal princípio;

b) Assegurar que os recursos colocados à disposição dos funcionários sejam utilizados apenas para as finalidades aprovadas pela empresa;

c) Garantir a continuidade do processamento das informações críticas ao negócio, seguindo a política específica para esse propósito;

d) Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual e as atividades do Grupo e seu mercado de atuação;

e) Determinar os mecanismos de Segurança da Informação, balanceando fatores de risco, tecnologia e custo.

8. DIRETRIZES

8.1. Da Informação

Todos os ativos de informação devem receber um nível adequado de proteção. Toda informação de propriedade do Grupo Mercantil é classificada para indicar a importância, a propriedade e o nível de proteção adequado.

Cada uma das informações criadas ou derivadas dos processos de negócios ou dos sistemas de suporte do Mercantil são de propriedade do Grupo e devem ter sua confidencialidade, integridade e disponibilidade protegidas.

Os recursos de Tecnologia da Informação possuem níveis de proteção compatíveis com a sua importância estratégica.

São adotados controles para prevenir e detectar a introdução de software malicioso ou quaisquer outras derivações de ataques digitais que possam surgir.

8.2. Da Organização e dos Controles Gerais de Segurança da Informação

A estrutura funcional para gerenciar a segurança dentro da organização é a responsável por iniciar e controlar a implantação dos controles específicos, nos quais são estabelecidos, entre outros:

- Manutenção da segurança da informação, quando a responsabilidade pelo processamento da informação é terceirizada;
- Monitoração dos riscos provenientes dos contratos de terceirização, considerando riscos, controles de segurança e procedimentos para os sistemas de informação, rede de computadores e/ou estações de trabalho;
- Prevenção contra danos aos ativos e interrupções das atividades do negócio;
- Proteção física das mídias de informação e dos sistemas de suporte aos negócios;
- Prevenção contra fraudes, perdas, modificações ou mau uso de informações trocadas entre organizações ou com clientes, em conformidade com a legislação pertinente;
- Garantia da segurança da informação, quando se utilizam a computação móvel e os recursos de trabalho remoto. A proteção requerida deve ser proporcional aos riscos desta forma específica de trabalho;
- Manutenção da segurança dos recursos de processamento de informação e ativos de informação organizacionais acessados por prestadores de serviço;
- Adoção de controles, de forma a prevenir exposição, perda, dano ou roubo de informação e de recursos de processamento da informação;
- Uso de criptografia para proteger a confidencialidade, autenticidade e integridade das informações;
- Garantia de que a segurança seja parte integrante dos sistemas de informação. Deve ser assegurado que todos os requisitos de segurança, incluindo a necessidade de acordos de contingência, sejam identificados na fase de levantamento de requisitos de um projeto e justificados, acordados e documentados como parte do estudo de caso de um negócio para um sistema de informação;
- Prevenção à perda, modificação ou ao uso impróprio de dados do usuário, nos sistemas de aplicações. Esses controles devem ser implementados na forma de trilhas de auditoria ou registro de atividades;
- Prevenção a acessos não autorizados e estabelecimento de procedimentos rígidos de controle de concessão de direitos de acesso aos sistemas de informação de negócios, aos sistemas operacionais, à rede de comunicação de dados, aos ambientes de desenvolvimento e de suporte do ambiente tecnológico, aos serviços de canais e aos arquivos dos sistemas;

- Acompanhamento das atividades e dos acessos não autorizados a sistemas aplicativos, sistemas operacionais e rede de comunicação de dados interna e externa. Faz-se necessário que os sistemas sejam monitorados, a fim de detectar divergências entre a política de controle de acesso e os registros de eventos monitorados, fornecendo evidências no caso de incidentes de segurança;

- Realização de testes de vulnerabilidade nos sites e aplicações móveis disponibilizadas na Internet para clientes e parceiros de negócios.

- Aderência a certificações exigidas para a prestação de serviços, quando aplicável.

- Documentação e monitoração dos mecanismos que implementam e garantem a efetividade das regras de segurança, procedimentos e controles internos.

- Identificação e segregação dos dados de clientes, funcionários e terceiros, utilizando controles físicos ou lógicos.

- Aderência legal ao Oficio-Circular nº 1/2024/CVM/SMI, assumindo o dever de zelar pela integridade e regular funcionamento do mercado e o dever de monitorar continuamente as operações e ofertas por ele intermediadas, de maneira a identificar situações de atipicidades, fraudes e de operações potencialmente irregulares cursadas nos mercados de valores mobiliários, mercado de bolsa e mercado de balcão organizado, nos termos do art. 33 da Resolução CVM nº 35/21.

8.3. Da Contingência e Continuidade de Negócios

O gerenciamento das redes interna e externa de comunicação de dados tem como premissa a garantia da salvaguarda das informações na rede, a proteção da infraestrutura de suporte e o desempenho e a disponibilidade da informação.

Os recursos e as instalações de processamento de informações críticas do negócio são mantidos em áreas seguras e padronizadas, a fim de evitar acesso não autorizado, dano e/ou interferência nas informações e instalações do Grupo.

Os dispositivos destinados à proteção das instalações físicas corporativas servem, também, como alternativas para contingências, em todos os segmentos vitais do negócio. As atividades do negócio, os processos críticos e os equipamentos são protegidos contra interrupções das atividades, sejam elas decorrentes de falhas, crises ou desastres.

São estabelecidos procedimentos de execução, retenção e salvaguarda de recursos, para viabilizar a restauração do ambiente em tempo hábil, conforme definido na estratégia de contingência para todos os níveis de processos considerados críticos.

Todo ambiente de contingência contemplado deve garantir sua permanente funcionalidade por meio de planos periódicos de simulação.

8.4. Da Conformidade

O projeto, a operação, o uso e a gestão dos sistemas de informação do Grupo Mercantil deverão estar em conformidade com os requisitos legais, sendo vedada a violação de qualquer lei criminal ou civil, estatuto, regulamentação, obrigação contratual ou requisito de segurança.

A atual Política de Segurança da Informação deve estar sempre em consonância com as regulamentações federais e aderente à Lei 12.965, denominada Marco Civil da Internet.

8.5. Da Segurança em Recursos Humanos

Assegurar que os usuários estejam cientes de suas responsabilidades, para a manutenção efetiva dos controles de acesso, considerando, particularmente, o uso de senhas e a segurança de seus equipamentos.

Reduzir os riscos de erro humano, roubo, fraude ou uso indevido das instalações, assegurando que as responsabilidades com a segurança sejam atribuídas na fase de recrutamento, incluídas em contratos e monitoradas durante a vigência de cada contrato de trabalho.

Assegurar que os usuários estejam cientes das possíveis ameaças tecnológicas e do risco do uso indevido de suas credenciais ou informações durante a execução normal do seu trabalho. Os usuários são treinados quanto aos procedimentos de segurança tecnológica e no uso correto das instalações de processamento da informação, de forma a minimizar possíveis riscos de segurança.

8.6. Dos Incidentes de Segurança

Todos os funcionários, conhecendo qualquer ato ilícito decorrente de falha no esquema de segurança adotado pelo Banco, devem notificar, exclusivamente, à área gestora de Segurança da Informação, via telefone ou enviando um e-mail para evidencia@mercantil.com.br.

Todos os incidentes de segurança deverão ter o seu registro efetivado, imediatamente, através do aplicativo de Gestão de Incidentes, sendo a área demandante notificada da abertura e do fechamento via e-mail.

8.7. Da Gestão de Ativos de Informação

Manter a proteção adequada dos ativos de informação da organização. Todos os principais ativos de informação, sejam sistemas e processos de negócios ou informações eletrônicas, são, periodicamente, inventariados e relacionados em sistema próprio, além de possuírem, também, um proprietário responsável na área de negócios, o qual deverá deliberar sobre acessos e quaisquer outros itens que envolvam o uso ou manuseio dos mesmos.

8.8. Da Segurança Física e do Ambiente

São prevenidos o acesso não autorizado, o dano e a interferência nas informações e nas instalações físicas da organização.

Os recursos e as instalações de processamento de informações críticas ou sensíveis do negócio são mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso.

8.9. Do Gerenciamento de Operações e Comunicações

Deve-se garantir a salvaguarda das informações na rede e a proteção da infraestrutura de suporte. O gerenciamento de segurança de rede que se estenda além dos limites físicos da organização requer particular atenção.

É importante que os procedimentos e informações operacionais estejam bem definidos, a fim de garantir que os recursos de processamento da informação sejam operados de forma segura e correta.

8.10. Da Aquisição, do Desenvolvimento e da Manutenção de Sistemas de Informação

O planejamento e a formalização do aceite de operação dos sistemas são fundamentais para minimizar o risco de falhas nos mesmos e são parte integrante dos processos ao qual o mesmo esteja inserido. Projeções de demanda de recursos e de carga de máquina futura devem ser feitas para reduzir o risco de sobrecarga dos sistemas.

É fundamental garantir que a aquisição e o desenvolvimento de sistemas estejam plenamente alinhados com os objetivos de negócios da Instituição, quanto aos seus requisitos de negócios e de segurança e quanto ao prazo de implantação.

9. PAPÉIS E RESPONSABILIDADES

Os papéis e responsabilidades atinentes a esta Política estão distribuídos entre as alçadas abaixo indicadas:

- Vice-Presidência de Produtos, Tecnologia e Serviços;
- Gerência de Segurança Cibernética e Informação;
- Todos os colaboradores;
- Terceiros
    - Ter ciência e pautar sua atuação conforme regras e diretrizes estabelecidas nesta Política.

10. CONSIDERAÇÕES FINAIS

Esta Política deve ser objeto de avaliação mínima bienal, com o intuito de que seja continuamente aprimorada e de que esteja sempre atualizada.

Este documento entra em vigor a partir de sua publicação, ficando à disposição dos órgãos de fiscalização e supervisão.

GRUPO MERCANTIL