



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

meu**tudo.**



SUMÁRIO

1. OBJETIVO	4
2. DEFINIÇÕES	4
3. ABRANGÊNCIA	10
4. PRINCÍPIOS E DIRETRIZES	11
5. PAPÉIS E RESPONSABILIDADES	12
5.1. DIRETORIA EXECUTIVA	12
5.2. CISO	12
5.3. COMITÊ DE SEGURANÇA DA INFORMAÇÃO	13
5.4. DPO/ENCARREGADO	14
5.5. TIME DE SEGURANÇA DA INFORMAÇÃO	15
5.6. TIMES DE TI	16
5.7. COMPLIANCE	16
5.8. CONTROLES INTERNOS	17
5.9. AUDITORIA INTERNA	17
5.10. COLABORADORES	17
5.11. TERCEIROS	17
6. GESTÃO DE RISCOS	18
7. CLASSIFICAÇÃO DA INFORMAÇÃO	18
8. GESTÃO DE ACESSOS	19
9. SEGURANÇA DE ATIVOS E DISPOSITIVOS	25
9.1. COMPUTADORES E RECURSOS TECNOLÓGICOS	25
9.2. DISPOSITIVOS MÓVEIS E BYOD	25
9.3. HARDENING E BASELINES DE CONFIGURAÇÃO	26
9.4. PROTEÇÃO DE REDE	26
9.5. SEGURANÇA FÍSICA	27
10. SEGURANÇA NA NUVEM E TRABALHO REMOTO	27
10.1. CLOUD COMPUTING	27
10.2. TRABALHO REMOTO	28
11. BACKUP E CONTINUIDADE DE NEGÓCIOS	29
11.1. BACKUP	29
11.2. PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)	29
12. GESTÃO DE VULNERABILIDADES E DESENVOLVIMENTO SEGURO	30
12.1. GESTÃO DE VULNERABILIDADES	30
12.2. DESENVOLVIMENTO SEGURO (DEVSECOPS)	31
13. CRIPTOGRAFIA E GESTÃO DE CHAVES	32
14. PROTEÇÃO DE AMBIENTES CRÍTICOS	33

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		



15. CYBER THREAT INTELLIGENCE E MONITORAMENTO	35
16. GESTÃO DE INCIDENTES DE SEGURANÇA	35
16.1. COMUNICAÇÃO REGULATÓRIA	36
16.2 PLAYBOOKS E ANÁLISE PÓS-INCIDENTE	36
17. GESTÃO DE TERCEIROS E TPRM	37
17.1 CLASSIFICAÇÃO DE TERCEIROS (TIERING) E INVENTÁRIO	37
17.2 DUE DILIGENCE PRE-CONTRATAÇÃO	39
17.3 REQUISITOS CONTRATUAIS MÍNIMOS	40
17.4 GESTÃO DE ACESSOS DE TERCEIROS	41
17.5 MONITORAMENTO CONTÍNUO	42
17.6 RESPOSTA A INCIDENTES COM VETOR EM TERCEIRO	42
17.7 CONCENTRAÇÃO DE RISCO E ESTRATÉGIA DE SAÍDA	43
18. CONSCIENTIZAÇÃO E TREINAMENTO DE SEGURANÇA	44
19. MONITORAMENTO, RELATÓRIO ANUAL E MELHORIA CONTÍNUA	44
20. VIGÊNCIA DA POLÍTICA	45
21. HISTÓRICO DE ALTERAÇÕES	45
22. REFERÊNCIAS NORMATIVAS	45
22.1. REGULAMENTAÇÃO	46
22.2. NORMAS TÉCNICAS	46
22.3. FRAMEWORKS E BOAS PRÁTICAS	46

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

1. OBJETIVO

Este documento (“Política”) tem por objetivo estabelecer as diretrizes, princípios e responsabilidades relativos à Segurança da Informação e Cibernética da Tudo Holding S.A., e as empresas por ela controladas, direta ou indiretamente, visando garantir a confidencialidade, integridade, disponibilidade e autenticidade de seus dados, sistemas e infraestruturas. A Política busca promover a ciber-resiliência institucional em linha com as melhores práticas de mercado, considerando a natureza, o porte, perfil de risco e a complexidade de nossos produtos, serviços, atividades, processos e sistemas, bem como a estrita conformidade aos requisitos legais e regulatórios aplicáveis.

2. DEFINIÇÕES

Para efeitos desta Política, as seguintes definições, quando aparecem com sua letra inicial em maiúsculo, no singular ou plural, terão os significados assinalados abaixo:

- **AIPD / DPIA / RIPD:** Relatório de Impacto à Proteção de Dados Pessoais (Art. 38 da LGPD). Obs.: o documento usa as três siglas de forma intercambiável — vale padronizar para uma só.
- **ANPD (“Autoridade Nacional de Proteção de Dados”):** Autarquia federal de natureza especial, dotada de autonomia técnica e decisória, responsável por zelar pela proteção de dados pessoais, fiscalizar o cumprimento da Lei Geral de Proteção de Dados (LGPD) e aplicar as sanções administrativas em caso de descumprimento da legislação no território nacional.
- **API (Application Programming Interface):** interface de comunicação entre sistemas.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

- **Ativo de Informação:** qualquer dado, sistema, equipamento, software, processo ou pessoa que tenha valor para a Instituição e que necessite de proteção contra riscos de segurança da informação.
- **Banco Central do Brasil (“BCB”):** principal órgão regulador e fiscalizador das instituições financeiras.
- **BYOD (Bring Your Own Device):** uso de dispositivos pessoais para acesso a recursos corporativos.
- **BYOK (Bring Your Own Key):** modelo no qual a organização gera e mantém o controle exclusivo das próprias chaves criptográficas, inclusive em nuvem.
- **CISO (Chief Information Security Officer):** Diretor de Segurança da Informação, responsável pela implementação, gestão e supervisão da política de segurança cibernética da Instituição perante a Diretoria Executiva e os reguladores.
- **Companhia (ou Instituição):** Refere-se à Tudo Holding S.A. e a todas as suas empresas controladas, direta ou indiretamente.
- **CMDB (Configuration Management Database):** base de dados de inventário e configuração de ativos.
- **Colaborador:** qualquer pessoa que tenha envolvimento profissional com a Instituição, incluindo membros do conselho, diretores, administradores, gerentes, empregados, funcionários, terceirizados, estagiários e jovens aprendizes.
- **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, nos termos do Art. 5º, inciso VI da LGPD. A Instituição atua como controladora nas operações de tratamento de dados pessoais de seus clientes e colaboradores.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

- **CTI (Cyber Threat Intelligence):** inteligência de ameaças cibernéticas; coleta, análise e disseminação de informações sobre ameaças para apoiar a defesa.
- **Dado Pessoal:** informação relacionada a pessoa natural identificada ou identificável, nos termos do Art. 5º, inciso I da LGPD.
- **Dado Pessoal Sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, nos termos do Art. 5º, inciso II da LGPD.
- **DevSecOps:** integração de práticas de segurança ao ciclo de desenvolvimento e operação de software.
- **DLP (Data Loss Prevention):** prevenção contra vazamento de dados; conjunto de tecnologias e controles que monitoram e impedem a exfiltração não autorizada de informações.
- **DPO / Encarregado:** Encarregado pelo Tratamento de Dados Pessoais, pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), conforme Art. 41 da LGPD.
- **EDR/XDR (Endpoint/Extended Detection and Response):** solução de segurança que monitora continuamente endpoints e outros ativos de TI para detectar, investigar e responder a ameaças cibernéticas em tempo real.
- **Hardening:** processo de configuração segura de sistemas conforme baselines (ex.: CIS Benchmarks).
- **HSM (Hardware Security Module):** dispositivo criptográfico dedicado e certificado para geração, armazenamento e proteção de chaves.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		



- **IAM (Identity and Access Management):** conjunto de processos, políticas e tecnologias para gerenciar identidades digitais e controlar o acesso de usuários a sistemas, aplicações e dados.
- **Incidente de Segurança:** qualquer evento confirmado ou sob suspeita que comprometa a confidencialidade, integridade ou disponibilidade das informações da Instituição, incluindo incidentes que envolvam dados pessoais de titulares.
- **IOC (Indicador de Comprometimento):** artefato observável (IP, domínio, hash, etc.) que indica atividade maliciosa.
- **MFA (Multi-Factor Authentication):** autenticação multifator, mecanismo de segurança que exige dois ou mais fatores de verificação de identidade para concessão de acesso a sistemas ou dados.
- **Open Finance (“OpF”):** ecossistema regulado pelo Banco Central do Brasil que permite o compartilhamento de dados e serviços financeiros entre instituições autorizadas, nos termos da Resolução Conjunta BACEN/CMN nº 1/2020.
- **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, nos termos do Art. 5º, inciso VII da LGPD.
- **PAM (Privileged Access Management):** solução e conjunto de controles destinados a gerenciar, monitorar e proteger o acesso privilegiado (administrativo) a sistemas, infraestruturas e dados críticos.
- **PCN:** Plano de Continuidade de Negócios. (Já vem expandido no título da seção, mas não tem entrada nas Definições.)
- **Pentest (Teste de Intrusão):** avaliação ofensiva controlada para identificar e explorar vulnerabilidades.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		



- **Pix:** arranjo de pagamentos instantâneos instituído e gerido pelo Banco Central do Brasil.
- **RoPA:** Registro das Operações de Tratamento de dados pessoais (Art. 37 da LGPD).
- **RPO (Recovery Point Objective):** ponto de recuperação objetivo — define a quantidade máxima aceitável de dados que podem ser perdidos em caso de incidente, expressa em unidade de tempo.
- **RSFN (Rede do Sistema Financeiro Nacional):** rede de comunicação de dados que interliga as instituições financeiras, o Banco Central e as câmaras/prestadores do SPB.
- **RTO (Recovery Time Objective):** tempo de recuperação objetivo — define o tempo máximo aceitável para restauração de um serviço ou sistema após uma interrupção.
- **SAST / SCA / IaC:** análise estática de código / análise de composição de software (dependências) / infraestrutura como código.
- **SGSI:** Sistema de Gestão de Segurança da Informação (ISO/IEC 27001).
- **SIEM (Security Information and Event Management):** plataforma de gerenciamento centralizado de eventos e informações de segurança, que coleta, correlaciona e analisa logs de múltiplas fontes para detectar ameaças em tempo real.
- **SLA (Service Level Agreement):** acordo de nível de serviço.
- **SPB (Sistema de Pagamentos Brasileiro):** conjunto de entidades, sistemas e procedimentos relacionados à transferência de recursos e à liquidação de operações financeiras no país.
- **STR (Sistema de Transferência de Reservas):** sistema de liquidação bruta em tempo real operado pelo Banco Central do Brasil para transferências interbancárias.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

- **Terceiros:** qualquer pessoa, seja ela prestador de serviços, representante, fornecedor, parceiro, consultor, dentre outros, que tenha envolvimento profissional ou comercial, ainda que transitório, com a Instituição, agindo em seu nome, atuando em conjunto com a empresa, nas dependências desta ou como preposto dela.
- **Tier (nível de criticidade de terceiro):** classificação atribuída a terceiros da Instituição com base no risco de segurança da informação que representam, variando de Tier 1 (Crítico) a Tier 4 (Baixo), conforme definido na Seção 20A desta política.
- **Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, nos termos do Art. 5º, inciso V da LGPD.
- **TLS / mTLS:** Transport Layer Security e sua variante com autenticação mútua, usados para proteger comunicações.
- **TPRM (Third Party Risk Management):** processo estruturado e contínuo de gestão dos riscos de segurança da informação originados por terceiros que fornecem produtos, serviços ou dados à Instituição, conforme detalhado na Seção 20A desta política.
- **Usuário:** toda pessoa que, de forma autorizada, acesse ativos de informação da Instituição.
- **VPN / VPC:** rede privada virtual / nuvem privada virtual (segmento isolado em provedor de nuvem).
- **WAF (Web Application Firewall):** firewall de aplicação web.
- **Zero Trust:** modelo de segurança que opera sob o pressuposto de que nenhum usuário, dispositivo ou conexão é confiável por padrão, independentemente de sua localização de rede, exigindo verificação contínua de identidade, postura do dispositivo e contexto para cada acesso.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

3. ABRANGÊNCIA

Esta Política aplica-se à Tudo Holding S.A. e às empresas por ela controladas, direta ou indiretamente, denominadas em conjunto neste documento como "meutudo" ou "Companhia"

Aplica-se de forma obrigatória a todos os envolvidos no ecossistema de negócios da Instituição, sejam Colaboradores em qualquer vínculo (CLT, PJ, estágio, aprendizagem, conselheiros e diretores), Terceiros, Parceiros, Fornecedores e Prestadores de Serviços (incluindo provedores de infraestrutura em nuvem).

4. PRINCÍPIOS E DIRETRIZES

A Segurança da Informação na Instituição é estruturada sobre os seguintes princípios fundamentais:

- Confidencialidade: a informação é acessível somente a quem esteja autorizado;
- Integridade: exatidão e completeza das informações e métodos de processamento são salvaguardadas;
- Disponibilidade: usuários autorizados têm acesso à informação e aos sistemas quando necessário;
- Autenticidade: informações e processos são genuínos e rastreáveis, objetivando assegurar a segurança das informações sensíveis.
- Menor Privilégio: todo acesso é restrito ao estritamente necessário para o desempenho da função;
- Segregação de Funções: responsabilidades incompatíveis são separadas para reduzir riscos de fraude ou erro;
- Responsabilização (Accountability): toda ação sobre informações e sistemas é rastreável;

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

- Privacidade por Design: proteção de dados pessoais incorporada desde a concepção de produtos e processos.
- Privacidade por Design: a proteção de dados pessoais é incorporada desde a concepção de produtos e processos.
- Zero Trust: nenhum usuário, dispositivo ou conexão é confiável por padrão; a verificação é contínua e contextual.

A Instituição reserva-se o direito de monitorar, auditar e inspecionar continuamente seus ambientes tecnológicos, redes, sistemas e dispositivos corporativos, visando a prevenção a fraudes, a detecção de ameaças cibernéticas e a proteção de dados. As regras de coleta e retenção de logs são disciplinadas em procedimento normativo específico.

O uso de ferramentas de software não homologadas (Shadow IT) e de serviços de inteligência artificial generativa é permitido somente mediante aprovação formal da área de TI e Segurança da Informação. É vedado inserir dados confidenciais, código-fonte proprietário ou dados de clientes em ferramentas de IA não homologadas.

5. PAPÉIS E RESPONSABILIDADES

5.1. DIRETORIA EXECUTIVA

- Garantir o suporte e o comprometimento da alta administração com os programas de Segurança da Informação.
- Aprovar e rever periodicamente esta Política de Segurança da Informação e o Plano de Ação de Resposta a Incidentes.
- Assegurar que os recursos necessários para a implementação da PSI estejam disponíveis.
- Tomar decisões estratégicas sobre investimentos em segurança.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

5.2. CISO

- Atuar como responsável executivo pela segurança da informação e cibernética, exercendo a função de diretor formalmente designado perante o Banco Central e respondendo à Diretoria e ao Comitê de Segurança da Informação pela definição, aprovação e manutenção desta política e do programa de segurança da Instituição.
- Definir e manter a estratégia, os controles e os indicadores de segurança, assegurar aderência às exigências legais e regulatórias.
- Supervisionar a gestão de riscos cibernéticos, liderar a resposta a incidentes relevantes e assegurar a comunicação tempestiva à Diretoria, ao Comitê e aos reguladores, nos prazos aplicáveis.
- Apresentar à Diretoria e ao Comitê o relatório anual e os relatórios operacionais periódicos — incidentes, pentests, vulnerabilidades por criticidade, testes de continuidade e indicadores de conformidade —, com vistas à promover a evolução contínua do programa.

5.3. COMITÊ DE SEGURANÇA DA INFORMAÇÃO

- Definir e revisar periodicamente as diretrizes estratégicas de Segurança da Informação, para assegurar alinhamento com os objetivos da organização.
- Acompanhar e avaliar os indicadores de segurança, incidentes relevantes e resultados de auditorias internas e externas.
- Aprovar planos de ação para mitigação de riscos identificados, e sua priorização, conforme critérios internos de impacto e criticidade.
- Apoiar a Diretoria Executiva na tomada de decisões estratégicas relacionadas à segurança da informação.
- Avaliar a eficácia da PSI e recomendar atualizações ou melhorias contínuas.
- Promover a integração entre as áreas da organização para assegurar que responsabilidades e controles de segurança estejam bem distribuídos.

12

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		



- Realizar reuniões periódicas para acompanhamento da maturidade em segurança da informação e conformidade regulatória.

5.4. DPO/ENCARREGADO

- Manter canais de comunicação com titulares e ANPD. Atuar como ponto focal entre a Instituição, os titulares de dados e a Autoridade Nacional de Proteção de Dados, recebendo, registrando e respondendo a solicitações, reclamações e requisições no âmbito da LGPD.
- Atender aos direitos dos titulares e assegurar o tratamento tempestivo dos pedidos de exercício de direitos (acesso, correção, anonimização, portabilidade, eliminação, revogação de consentimento), prestando os esclarecimentos e adotando as providências cabíveis.
- Assegurar a Governança de privacidade e conformidade. Orientar colaboradores e terceiros sobre boas práticas de proteção de dados. Manter o Registro das Operações de Tratamento (ROPA) e apoiar a elaboração dos Relatórios de Impacto à Proteção de Dados (RIPD/DPIA), em observância às diretrizes da Lei Geral de Proteção de Dados (LGPD).
- Assegurar a resposta a incidentes com dados pessoais em conjunto com o CISO e o Time de Segurança da Informação, em observância aos incidentes que envolvam dados pessoais, além de conduzir a comunicação à Agência Nacional de Proteção de Dados (ANPD) e aos titulares afetados, nos prazos e formatos aplicáveis.

5.5. TIME DE SEGURANÇA DA INFORMAÇÃO

- Definir, implementar e revisar os controles de segurança da rede, garantindo a proteção do ambiente de dados dos titulares de cartões.
- Implementar criptografia para dados armazenados, monitorando o acesso para que apenas usuários autorizados acessem informações sensíveis.

13

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

- Assegurar que os dados dos titulares de cartão sejam protegidos por criptografia forte durante a transmissão em redes públicas ou abertas.
- Monitorar vulnerabilidades conhecidas, aplicar patches de segurança e gerenciar software de proteção contra malware em todos os sistemas da organização.
- Monitorar e garantir que os desenvolvimentos de software estejam aderentes às melhores práticas de segurança, incluindo revisões de código e testes de vulnerabilidades.
- Realizar treinamentos de segurança para conscientizar sobre a importância da segurança na Instituição.
- Supervisionar as atividades relacionadas à segurança da informação e garantir que estejam em conformidade com a PSI.
- Revisar regularmente os riscos de segurança
- Implementar melhorias contínuas no processo de segurança.
- Avaliar incidentes de segurança e garantir que medidas corretivas sejam tomadas.
- Implementar e coordenar as práticas de segurança da informação.
- Desenvolver e manter a Política de Segurança da Informação atualizada.
- Garantir a conformidade com normas e regulamentações externas de segurança.
- Coordenar auditorias internas e externas sobre a temática de Segurança da Informação.
- Gerenciar incidentes de segurança com resposta rápida e efetiva.

5.6 TIMES DE TI

- Implementar e manter os controles técnicos de segurança em seus respectivos domínios.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		



- Seguir os processos formais de gestão de mudanças e desenvolvimento seguro.
- Realizar avaliações de vulnerabilidade e garantir a aplicação tempestiva de patches.
- Gerenciar backups e restaurar dados de forma segura, conforme RPO e RTO definidos.

5.7. COMPLIANCE

- Verificar a aderência às normas regulatórias frente à temática de Segurança da Informação.
- Realizar a comunicação com os órgãos reguladores, conforme necessidade.

5.8. CONTROLES INTERNOS

- Realizar a análise do ambiente de controles internos sobre a temática de Segurança da Informação, conforme preceitua a Resolução CMN nº 4.968/2021, além de testes de efetividade de controles, em linha com as melhores práticas de mercado e diretrizes internas.

5.9. AUDITORIA INTERNA

- Realizar auditorias periódicas para verificar a aderência a esta Política e às legislações legais e infralegais vigentes.

5.10. COLABORADORES

- Seguir as diretrizes da PSI e relatar quaisquer Incidentes ou suspeitas de violação de segurança.
- Utilizar os recursos de TI de forma responsável.
- Participar de treinamentos periódicos sobre segurança da informação.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

5.11. TERCEIROS

- Cumprir as normas de segurança estabelecidas no contrato e na PSI.
- Assegurar que os serviços prestados estejam em conformidade com os requisitos de segurança da organização.
- Relatar qualquer incidente de segurança relacionado aos serviços prestados.

6. GESTÃO DE RISCOS

A Instituição adota processo formal, contínuo e documentado de gestão de riscos de segurança da informação, integrado a estrutura de gerenciamento de riscos operacionais e de continuidade de negócios.

O processo de avaliação de riscos utiliza metodologia documentada e reproduzível, contemplando:

- Critérios de aceitação de risco aprovados pelo Conselho de Administração ou Diretoria.
- Identificação de proprietários dos riscos e avaliação periódica com base em ameaças e vulnerabilidades.
- Plano de tratamento de riscos formalmente aprovado.
- Implementação de controles para mitigar riscos identificados.
- Análise específica dos riscos associados à contratação de serviços de terceiros e computação em nuvem.
- Realização de Avaliações de Impacto a Proteção de Dados (AIPD/DPIA) para atividades de alto risco, aprovadas pelo DPO.
- Monitoramento contínuo e revisão dos riscos e controles.
- Definição de um plano de resposta a incidentes.
- Treinamento e conscientização sobre segurança da informação para colaboradores.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

A gestão de riscos é revisada com periodicidade mínima anual e sempre que ocorrerem mudanças significativas no ambiente tecnológico, regulatório ou de negócios.

7. CLASSIFICAÇÃO DA INFORMAÇÃO

Toda a informação produzida, recebida ou custodiada pela instituição deve ser classificada de acordo com sua sensibilidade e criticidade, definindo os controles de acesso, tratamento, armazenamento e descarte adequados.

São definidos formalmente os seguintes níveis de classificação da informação, com critérios objetivos e regras de tratamento, marcação, transferência e descarte para cada categoria, conforme controles 5.12 e 5.13 da ABNT NBR ISO/IEC 27001:2022: (1) Público; (2) Interno; (3) Confidencial; e (4) Restrito. As regras de tratamento para cada nível são detalhadas em norma específica. A Instituição implanta e opera mecanismos de prevenção de vazamento de informações (DLP), com escopo atinente aos serviços Google.

Dados pessoais sensíveis (LGPD, Art. 11) são classificados, no mínimo, como Confidencial, implicando criptografia e controles de acesso obrigatórios. Informações financeiras de clientes observam o nível mínimo de confidencialidade, nos termos da Lei Complementar no 105/2001 (sigilo bancário).

A Instituição mantém Registro de Operações de Tratamento de Dados Pessoais (ROPA), com mapeamento da finalidade, base legal, categorias de dados, prazo de retenção e medidas de segurança para cada atividade, em observância às diretrizes da LGPD.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

8. GESTÃO DE ACESSOS

A gestão de acessos baseia-se nos princípios do Menor Privilégio (acesso restrito ao estritamente necessário para a função) e da Segregação de Funções e Zero Trust. Todo o acesso aos ativos de informação são de uso pessoal e intransferível. O compartilhamento de credenciais constitui infração grave, sujeita a medidas disciplinares e legais.

8.1. AUTENTICAÇÃO E GESTÃO DE IDENTIDADE

A Instituição adota MFA como requisito obrigatório para acesso a sistemas críticos, dados de clientes e ambientes de produção. Acessos remotos a sistemas com dados de clientes ou infraestrutura crítica requerem MFA resistente a phishing.

A renovação de senhas baseia-se primordialmente em eventos de risco — suspeita ou confirmação de comprometimento de credencial — evitando-se a rotação periódica forçada que possa induzir a criação de senhas previsíveis. Os parâmetros técnicos de composição, histórico e bloqueio por inatividade são definidos em norma específica de Gestão de Acessos.

Adicionalmente, são distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme requisitos mínimos estabelecidos em norma específica.

- **14 (quatorze) caracteres alfanuméricos**
- **Utilizando caracteres especiais (!, @, #, \$, %, &, *)**

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

- **Variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo).**

É de responsabilidade de cada Colaborador a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após 3 (três) tentativas de acesso, a conta do Colaborador será bloqueada. Para o desbloqueio é necessário que o Colaborador entre em contato com Suporte da Instituição. Ademais, deverá confirmar a identidade para a renovação de senha identidade.

Os Colaboradores podem alterar a própria senha, sendo orientados a fazê-lo caso haja suspeita de acesso indevido. O sistema operacional deve fazer o bloqueio de tela a partir de 05 (cinco) minutos de inatividade.

A periodicidade máxima para troca das senhas é 60 dias, não podendo ser repetidas as 5 (cinco) últimas senhas. Os sistemas críticos e sensíveis para com privilégios administrativos devem exigir a troca de senhas a cada 60 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum Colaborador for

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao Departamento de Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos Usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos Usuários de testes e outras situações similares.

O acesso com perfil de administrador (ADM) a sistemas, bancos de dados e infraestrutura é um privilégio concedido estritamente para a execução das atividades laborais inerentes ao cargo do Colaborador. Seu uso indevido representa uma quebra de confiança e uma falha grave de segurança em observância à finalidade de acesso.

O uso do acesso administrativo em desacordo com esta política será considerado ato de indisciplina e/ou insubordinação, podendo também configurar violação de segredo da empresa, a depender da natureza da informação acessada e poderá acarretar a aplicação de medidas disciplinares, conforme previsto na Política de Medidas Disciplinares da empresa.

8.2. CICLO DE VIDA DOS ACESSOS

- Provisionamento: acessos concedidos formalmente, com aprovação do gestor, vinculados à função exercida e documentados em sistema de IAM.
- Revisão periódica: perfis de acesso revisados semestralmente; acessos privilegiados, trimestralmente. A revisão de colaboradores terceirizados ocorre trimestralmente.
- Revogação imediata: em caso de desligamento, mudança de função ou incidente de segurança envolvendo o colaborador.
- Acessos de Terceiros: gerenciados com controles equivalentes ou superiores aos de colaboradores internos, com prazo determinado e

20

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		



MFA obrigatório. Todas as sessões de acesso remoto de terceiros são registradas em log retido por mínimo de 12 meses.

8.3. RASTREABILIDADE DE TRANSAÇÕES

A Instituição implementa mecanismos de rastreabilidade de transações e operações, contemplando trilhas de auditoria do processamento “fim a fim” dos dados, com geração de logs que possibilitam identificar falhas de processamento ou comportamentos atípicos.

A retenção de logs é realizada em observação à tabela abaixo:

Tipo de log / operação	Retenção mínima	Base normativa
Trilhas de auditoria de transações financeiras (Pix, STR)	5 anos	CMN 5.274/2025 · BCB 538/2025
Logs de acesso a sistemas e aplicações	5 anos	CMN 5.274/2025
Logs de acessos privilegiados / administrativos	5 anos	CMN 5.274/2025
Relatórios e evidências de pentest	5 anos	CMN 5.274/2025
Planos de ação de remediação de vulnerabilidades	5 anos	CMN 5.274/2025
Logs de incidentes de segurança	5 anos	CMN 5.274/2025 · LGPD
Reportes periódicos ao Comitê e à Diretoria	5 anos	CMN 5.274/2025
Registros de acesso — logs operacionais não críticos	6–12 meses	Marco Civil, Art. 13 · ISO 27001

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

Todo o período de guarda visa assegurar integridade, confidencialidade e disponibilidade e compreende: (i) armazenamento em repositório segregado com acesso restritivo; (ii) verificação de integridade (hash ou assinatura digital) nos registros de operações críticas; (iii) criptografia em repouso; (iv) disponibilidade imediata dos últimos 3 meses; e (v) auditorias semestrais de integridade e completude das trilhas.

9. SEGURANÇA DE ATIVOS E DISPOSITIVOS

A Instituição mantém inventário formal e continuamente atualizado de todos os seus ativos de informação (hardware, software, serviços em nuvem, APIs, dados e dependências), organizado em CMDB ou equivalente. Apenas ativos inventariados e aprovados podem operar na rede corporativa.

9.1 COMPUTADORES E RECURSOS TECNOLÓGICOS

Os recursos tecnológicos são de propriedade da Instituição e devem ser utilizados exclusivamente para fins corporativos. São vedados: tentativas de acesso não autorizado, uso de software não licenciado, instalação sem autorização da TI e alteração de configurações de sistemas operacionais sem autorização. Dispositivos são bloqueados automaticamente após no máximo 5 minutos de inatividade.

9.2 DISPOSITIVOS MÓVEIS E BYOD

O uso de dispositivos pessoais (BYOD) para acesso a sistemas e dados corporativos é permitido mediante aprovação prévia da TI, sujeito a: instalação de MDM, MFA obrigatório, criptografia de dados corporativos, separação entre dados pessoais e corporativos, antivírus atualizado e notificação imediata à TI em caso de furto, roubo ou comprometimento.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

O uso de dispositivos pessoais para tratamento de dados pessoais de clientes é controlado conforme o Art. 46 da LGPD e o controle 6.7 da ABNT NBR ISO/IEC 27001:2022.

9.3 HARDENING E BASELINES DE CONFIGURAÇÃO

Todos os sistemas operacionais, serviços e componentes de infraestrutura são configurados conforme baselines de segurança (referência: CIS Benchmarks) antes de entrar em produção. Desvios são tratados como vulnerabilidades. Software em fim de vida (EOL/EOS) é isolado e incluído em plano de substituição com prazo definido.

9.4 PROTEÇÃO DE REDE

A Instituição implementa e mantém controles de proteção da rede corporativa, abrangendo:

- Segmentação lógica e física da rede, resguardando o ambiente de produção e os recursos que suportam processos críticos.
- Estabelecimento e monitoramento contínuo de regras de firewall, bloqueando tentativas de conexão de ativos externos não autorizados.
- Critérios documentados para o estabelecimento e o monitoramento de conexões com ambientes externos, com atenção especial a conexões em horário noturno e em dias não úteis.
- Medidas para identificar e prevenir conexões indevidas com ambientes externos oriundos de recursos tecnológicos da Instituição.
- Restrição de acesso à rede corporativa apenas a dispositivos formalmente autorizados.
- VPN corporativa obrigatória para acesso remoto a sistemas internos, incluindo trabalho remoto e acessos externos de Terceiros.

A Instituição realiza varreduras automatizadas de descoberta de ativos com frequência mínima semanal na rede corporativa. Qualquer ativo fora

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

do inventário oficial é imediatamente isolado e investigado pelo Time de Segurança da Informação. O inventário é atualizado automaticamente a partir das varreduras e revisado manualmente de forma trimestral. Relatórios de varredura são retidos por no mínimo 5 anos.

9.5 SEGURANÇA FÍSICA

São definidos formalmente perímetros de segurança física, zonas de acesso controlado e procedimentos de proteção de equipamentos. Áreas com ativos sensíveis são monitoradas por sistemas de controle de acesso, incluindo controle biométrico ou por crachá para ambientes que suportam sistemas críticos de operações financeiras.

10. SEGURANÇA NA NUVEM E TRABALHO REMOTO

10.1 CLOUD COMPUTING

A contratação e o uso de serviços em nuvem observam os requisitos dos Arts. 13 a 20 da Resolução CMN nº 4.893/2021, incluindo:

- Política específica para contratação de serviços em nuvem, com avaliação de relevância e capacidade do prestador.
- Comunicação ao Banco Central do Brasil em até 10 dias após a contratação de serviços relevantes, informando denominação, serviços e países (Art. 15 da Res. CMN nº 4.893/21).
- Cláusulas contratuais mínimas obrigatórias, conforme Art. 17 da Res. CMN nº 4.893/21, incluindo: indicação de países de armazenamento, medidas de segurança, segregação de dados, procedimentos de extinção do contrato, acesso do BACEN a dados e infraestrutura, e vedação de subcontratação relevante sem anuência prévia.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

- Os requisitos de isolamento físico e lógico do ambiente STR são assegurados contratualmente quando o provedor opera esses ambientes, nos termos do Art. 3o-A, I, "b" e "c".

- Processos formais para aquisição, uso, gerenciamento e encerramento de serviços, incluindo estratégia de saída, portabilidade de dados e provedores alternativos avaliados previamente.

10.2 TRABALHO REMOTO

Colaboradores em regime remoto seguem as mesmas normas de segurança que os presenciais, com controles adicionais:

- Uso obrigatório de VPN corporativa para acesso a sistemas internos;
- Bloqueio de tela automático e proibição de uso de redes Wi-Fi públicas sem VPN;
- Restrição de impressão ou cópia de documentos confidenciais em ambientes externos.

É realizada avaliação de riscos específica para o trabalho remoto envolvendo dados pessoais sensíveis ou operações financeiras, documentada e revisada anualmente.

11. BACKUP E CONTINUIDADE DE NEGÓCIOS

11.1. BACKUP

A Instituição implementa gestão de cópias de segurança (backup) como controle mínimo obrigatório, nos termos do Art. 3o, §2o, VII, da Resolução CMN no 4.893/2021. Os backups são automatizados, realizados fora do horário comercial e armazenados em ambientes seguros, com cópias em localidade geograficamente distinta. Os procedimentos de backup são vinculados ao RTO e ao RPO definidos

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

no PCN para cada sistema crítico, documentados e revisados anualmente.

Testes de restauração são realizados com frequência definida conforme criticidade do sistema, com resultados documentados e critérios formais de aceitação. Falhas nos testes de restauração são tratadas como incidentes de segurança.

11.2 PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)

O PCN contempla:

Identificação dos serviços críticos e dos cenários de interrupções relevantes, incluindo cenários de incidentes cibernéticos.

- Definição documentada de RTO e RPO para cada serviço crítico, com critérios formais que configuram situação de crise.
- Estratégias de recuperação documentadas, testadas semestralmente e atualizadas conforme necessário.
- Comunicação formal e tempestiva ao Banco Central do Brasil em situações de crise.

Os testes de continuidade contemplam explicitamente cenários de indisponibilidade da RSFN, do Pix e do STR, com periodicidade mínima semestral e resultados reportados ao Comitê de Segurança da Informação e à Diretoria.

Toda alteração em ambientes de produção segue processo formal de gestão de mudanças, com categorização, análise de impacto e risco, aprovação, janela de manutenção e procedimento de rollback documentado. Mudanças emergenciais requerem aprovação retroativa em até 24 horas.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

12. GESTÃO DE VULNERABILIDADES E DESENVOLVIMENTO SEGURO

12.1 GESTÃO DE VULNERABILIDADES

A Instituição mantém processo formal de identificação, avaliação e tratamento de vulnerabilidades técnicas, abrangendo:

- Testes e análises periódicas para detecção de vulnerabilidades em sistemas de informação.
- Varreduras periódicas dos recursos tecnológicos para identificar dispositivos indevidamente conectados à rede corporativa.
- Análises periódicas com o objetivo de identificar vulnerabilidades que possam comprometer a segurança dos ativos.
- Testes de intrusão (pentests) com periodicidade mínima anual, realizados com independência e imparcialidade por empresa especializada contratada para essa finalidade, sem prejuízo de testes realizados por equipes internas.
- Correção tempestiva das vulnerabilidades identificadas, dentro dos prazos por criticidade estabelecidos internamente.

Documentação dos resultados dos pentests e das varreduras, com as vulnerabilidades identificadas e os planos de ação para correção, à disposição do Banco Central do Brasil pelo prazo de 5 anos.

Quando não houver correção disponível, são implementados controles alternativos temporários até a remediação definitiva. Patches são verificados e testados em ambiente de homologação antes de serem aplicados em produção, alinhados ao processo de gestão de mudanças.

12.2. DESENVOLVIMENTO SEGURO (DEVSECOPS)

O desenvolvimento de sistemas incorpora segurança em todas as etapas do ciclo de vida. Os controles abrangem:

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		



- Scanning automático de código (SAST) em cada pull request, bloqueando merges com vulnerabilidades críticas ou altas não tratadas.
- Análise de composição de software (SCA) para identificar dependências com vulnerabilidades conhecidas.
- Scanning de segredos em repositórios (impedindo commit de credenciais, tokens ou chaves).
- Scanning de imagens de container e infraestrutura como código (IaC) antes do deploy em produção.
- Segregação de ambientes de desenvolvimento, homologação e produção.
- Análise de requisitos de segurança para todo sistema que trate dados de clientes ou operações financeiras, antes do início do desenvolvimento;
- Verificação de requisitos de desenvolvimento seguro em sistemas adquiridos de Terceiros ou desenvolvidos por Terceiros e executados na infraestrutura da Instituição.

O desenvolvimento e a operação de APIs seguem as diretrizes da OWASP API Security Top 10 (2023), com autenticação e autorização robustas em todos os endpoints, rate limiting, validação de inputs/outputs, API gateway com WAF, e inventário centralizado de APIs com proprietário técnico designado.

É expressamente vedado o commit ou a promoção de código com segredo hardcoded para qualquer ambiente. Violações dessa regra são tratadas como incidentes de segurança.

13. CRIPTOGRAFIA E GESTÃO DE CHAVES

As chaves privadas de assinatura de mensagens Pix, STR e RSFN permanecem sob controle exclusivo da Instituição, armazenadas em cofre seguro, de modo a impedir o acesso do provedor de nuvem ao material

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

criptográfico. A integridade e a autenticidade de cada transação são validadas antes da assinatura, por mecanismo independente do canal de transmissão.

O uso de criptografia é obrigatório para dados sensíveis em trânsito e em repouso. São adotados, no mínimo, os seguintes padrões:

- Dados em trânsito: TLS 1.2 ou superior (preferencialmente TLS 1.3). APIs do Open Finance utilizam mTLS em endpoints sensíveis, com cipher suites aprovadas pelo Open Finance Brasil Security Profile.
- Dados em repouso: AES-256 ou equivalente para bases de dados, storage e backups com dados Confidenciais ou Restritos.
- Certificados digitais: adquiridos de Autoridade Certificadora confiável ou gerados internamente com RSA mínimo 2048 bits.

O ciclo de vida completo das chaves criptográficas é gerenciado formalmente, incluindo geração, distribuição, armazenamento, renovação, revogação e destruição segura (ABNT NBR ISO/IEC 27001:2022). Nenhuma chave privada permanece ativa além de seu prazo de validade sem aprovação formal.

As chaves privadas e segredos são armazenados em sistemas de gerenciamento de segredos (ex.: AWS Secrets Manager ou equivalente), com acesso restrito pelo princípio do menor privilégio e auditado continuamente.

A pseudonimização e anonimização são aplicadas sempre que tecnicamente viáveis.

14. PROTEÇÃO DE AMBIENTES CRÍTICOS

Aplica-se a todos os sistemas, componentes, pessoas e processos que interajam com o Pix, o STR, a RSFN e quaisquer sistemas que processem, transmitam ou armazenem mensagens financeiras estruturadas destinadas ao SPB. Constituem diretrizes mínimas:

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

Isolamento lógico e físico

- Os ambientes de produção do Pix e do STR são mantidos em segmentos de rede exclusivos, isolados por firewalls e controles de segmentação. O acesso é restrito ao mínimo de usuários necessários, com revisão semestral.
- No ambiente de nuvem, é aplicado isolamento equivalente ao on-premises, com VPC, security groups e IAM dedicados e auditados.
- Os testes, desenvolvimento e homologação do Pix ou STR, somente ocorrem em ambientes de teste e utilizam dados anonimizados.

Proteção de chaves criptográficas.

- As chaves privadas de assinatura de mensagens Pix, STR e RSFN permanecem sob controle exclusivo da Instituição e não podem ser exportadas, compartilhadas ou acessadas por terceiros, inclusive provedores de nuvem. O armazenamento utiliza HSM certificado ou solução equivalente, priorizando Cloud HSM com BYOK (Bring Your Own Key).
- Aspectos de integridade e autenticidade da transação são validadas por mecanismo independente do canal de transmissão Antes da assinatura de qualquer mensagem ao SPB.
- O ciclo de vida das chaves segue procedimento documentado e auditável, retido por no mínimo 5 anos

Controles adicionais e continuidade

- Contratos com provedores da cadeia de processamento na RSFN incluem cláusulas específicas de segurança, SLAs de disponibilidade e direito de auditoria.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

- Os cenários de indisponibilidade da RSFN, do Pix e do STR, com contingência são documentados, e testados e contemplados na Política de Continuidade de Negócios (PCN) da Instituição.
- Incidentes que afetem a RSFN são tratados como de alta criticidade e notificados ao Banco Central.
- Testes de continuidade específicos para Pix e STR são realizados semestralmente, com resultados reportados ao Comitê de Segurança da Informação e à Diretoria.

15. CYBER THREAT INTELLIGENCE E MONITORAMENTO

O programa de CTI segue ciclo estruturado: planejamento (definição de prioridades de inteligência — PIRs — a partir da Gestão de Riscos), coleta, processamento (correlação e contextualização em inteligência acionável), disseminação tempestiva às áreas competentes e ação/feedback.

O programa monitora campanhas de phishing e impersonation que utilizem a marca, os domínios ou a identidade visual da Instituição, visando identificar infraestrutura maliciosa associada a ataques direcionados.

Ademais, participa-se de grupos setoriais de compartilhamento de informações sobre incidentes com outras instituições, sem prejuízo do sigilo e da livre concorrência.

16. GESTÃO DE INCIDENTES DE SEGURANÇA

A Instituição mantém processo formal e estruturado de gestão de incidentes de segurança, abrangendo detecção, contenção, erradicação, recuperação, notificação regulatória e análise pós-incidente.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		



Colaboradores e Terceiros reportam imediatamente qualquer anomalia ou suspeita de incidente ao canal oficial: security@meutudo.app.

16.1. COMUNICAÇÃO REGULATÓRIA

Regulador	Evento	Prazo e Fundamento
Banco Central do Brasil	Incidente relevante (tipo, sistemas afetados, impacto e medidas adotadas)	Conforme Art. 9º da Resolução CMN nº 4.893/2021
ANPD	Incidente com dados pessoais que possa causar risco ou dano aos titulares	Comunicação preliminar em até 2 dias úteis após ciência (LGPD, Art. 48; Resolução CD/ANPD nº 15/2024)

16.2 PLAYBOOKS E ANÁLISE PÓS-INCIDENTE

A Instituição mantém playbooks documentados e testados semestralmente para os principais tipos de incidente (ransomware, comprometimento de credenciais, vazamento de dados e ameaça interna). Todo incidente relevante é encerrado com registro formal de lições aprendidas, análise de causa-raiz e proposição de controles preventivos, apresentados ao Comitê de Segurança da Informação.

O Plano de Ação e Resposta a Incidentes — é um documento distinto e complementar a esta Política, nos termos do Art. 6º da Resolução CMN nº 4.893/2021, contendo rotinas, procedimentos, controles e tecnologias para prevenção e resposta. O documento é revisado anualmente em conjunto com esta Política e aprovado pela Diretoria da Instituição.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

17. GESTÃO DE TERCEIROS E TPRM

A Instituição é responsável pela confiabilidade, integridade, disponibilidade, segurança e sigilo em relação aos dados de clientes mesmo quando o processamento é realizado por Terceiros. O programa de Gestão de Riscos de Terceiros (TPRM) é processo estruturado e contínuo de identificação, avaliação, tratamento e monitoramento dos riscos de segurança da informação originados por fornecedores, parceiros, prestadores de serviços e quaisquer partes externas que acessem, processem, armazenem ou transmitam dados da Instituição ou que forneçam componentes críticos à infraestrutura tecnológica.

17.1 CLASSIFICAÇÃO DE TERCEIROS (TIERING) E INVENTÁRIO

Todos os Terceiros são classificados em quatro níveis de criticidade, com base no tipo de acesso, volume e sensibilidade dos dados envolvidos, e criticidade do serviço para a continuidade operacional:

Tier	Criticidade	Perfil	Periodicidade
1	Crítico	Acesso direto a dados de clientes, sistemas produtivos ou infraestrutura crítica; ou cuja indisponibilidade impacta a operação. Terceiros identificados como ponto único de falha são automaticamente	Avaliação completa pré-contratação + reavaliação anual.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

Tier	Criticidade	Perfil	Periodicidade
		classificados como Tier 1.	
2	Alto	Acesso a sistemas internos sem dados de clientes, ou acesso eventual a informações confidenciais.	Avaliação simplificada para contratação + reavaliação anual.
3	Médio	Sem acesso direto a dados ou sistemas sensíveis, mas com impacto operacional relevante ou acesso físico às instalações.	Bienal.
4	Baixo	Sem acesso a dados ou sistemas da Instituição.	Autodeclaração anual.

A Instituição mantém inventário centralizado e continuamente atualizado de todos os Terceiros ativos, contendo: tier de risco, data da última avaliação, status de conformidade, owner interno, escopo de acesso concedido, vigência do contrato e certificações apresentadas. O inventário é revisado trimestralmente pelo CISO e reportado semestralmente ao Comitê de Segurança.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

17.2 DUE DILIGENCE PRE-CONTRATACAO

Nenhum Terceiro Tier 1 ou Tier 2 é contratado sem a conclusão do processo formal de due diligence de segurança. O processo abrange:

- Aplicação de questionário de segurança padronizado (referência: CAIQ da Cloud Security Alliance para provedores de cloud), cobrindo: política de SI, controles de acesso, criptografia, gestão de vulnerabilidades, resposta a incidentes, continuidade de negócios e conformidade regulatória.
- Verificação de certificações vigentes: Terceiros Tier 1 que processam dados de clientes apresentam certificação ISO 27001 válida ou relatório SOC 2 Type II emitido há no máximo 12 meses. A ausência de certificações implica due diligence aprofundada, podendo incluir visita técnica às instalações.
- Avaliação de conformidade com a LGPD para Terceiros que realizam processamento de dados pessoais, verificando: existência de política de privacidade, designação de DPO, histórico de incidentes e capacidade de atendimento aos direitos dos titulares. O resultado é documentado como evidência da diligência na seleção de operadores.
- Avaliação do plano de continuidade e da estratégia de saída, incluindo procedimento de portabilidade de dados, prazo estimado de migração e provedores alternativos previamente avaliados.
- Scoring quantitativo de risco com base nos domínios: controles técnicos (30%), governança de SI (20%), gestão de incidentes (20%), conformidade regulatória (20%) e continuidade (10%). Terceiros com score abaixo do limiar definido pelo Comitê de Segurança não são contratados sem aprovação explícita da Diretoria Executiva e plano de tratamento formalizado.
- Aprovação formal pelo CISO antes da assinatura do contrato.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

17.3 REQUISITOS CONTRATUAIS MÍNIMOS

Todos os contratos com Terceiros incluem cláusulas mínimas de segurança, proporcionais ao tier:

- Cláusulas universais (todos os tiers): cumprimento das políticas de SI da Instituição; notificação de incidentes em até 24 horas da identificação; direito de auditoria e solicitação de evidências de conformidade; confidencialidade perpétua sobre dados da Instituição e de seus clientes; penalidades por descumprimento; e responsabilidade solidária pelos danos causados por incidentes decorrentes do descumprimento contratual de segurança, com direito de regresso da Instituição.
- Cláusulas adicionais para Tier 1: garantia de acesso do BACEN às instalações, sistemas e informações do Terceiro; proibição de subcontratação relevante (quarteirização) sem anuência prévia por escrito; SLA de disponibilidade compatível com os RTO e RPO do PCN; procedimento documentado de encerramento e portabilidade de dados ao término do contrato; comunicação prévia de mudanças significativas na infraestrutura ou no time responsável.
- Cláusulas para operadores de dados pessoais: formalização da relação controlador-operador com finalidade, base legal e instruções documentadas de tratamento; proibição de transferência internacional de dados sem autorização prévia; obrigação de eliminação segura ao término do contrato; e obrigação de comunicar a Instituição qualquer solicitação de autoridade pública de acesso a dados de titulares, antes de atendê-la, salvo proibição legal.

17.4 GESTÃO DE ACESSOS DE TERCEIROS

Os acessos de Terceiros são gerenciados com controles equivalentes ou superiores aos aplicados a colaboradores da Instituição:

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

- Todos os acessos são nominais, individualizados e associados a um responsável identificado no Terceiro e a um interno na Instituição. São concedidos por prazo determinado, correspondente ao escopo da atividade contratada, e revisados mensalmente pelo owner interno.
- MFA é obrigatório para todos os acessos remotos. Acessos a sistemas produtivos ou dados de clientes requerem MFA resistente a phishing (FIDO2 ou certificado digital).
- Acessos a sistemas críticos ou infraestrutura de produção são realizados exclusivamente por solução do PAM, com gravação de sessão e aprovação just-in-time. Nenhum Terceiro mantém credenciais permanentes de acesso privilegiado. É expressamente vedado o acesso de Terceiros as chaves privadas de certificados de assinatura de mensagens da RSFN, conforme Art. 3o-A, alínea f, da Resolução CMN no 4.893/2021.
- Todas as sessões de acesso remoto são registradas em log com identificação do usuário, IP de origem, sistemas acessados, comandos executados e duração da sessão. Logs são retidos por mínimo de 12 meses.
- Acessos são revogados imediatamente ao término do contrato, conclusão do projeto, afastamento do colaborador do Terceiro ou em caso de incidente de segurança. O processo de offboarding de Terceiros segue o mesmo fluxo do offboarding de colaboradores da Instituição.

17.5 MONITORAMENTO CONTÍNUO

O monitoramento de Terceiros é proporcional ao tier:

- Tier 1: monitoramento contínuo por alertas de CTI (incidentes públicos, vulnerabilidades em produtos utilizados, sanções regulatórias); verificação semestral de certificações vigentes; análise dos relatórios de incidentes reportados pelo Terceiro; e revisão anual completa com novo questionário e relatório SOC 2 ou equivalente.
- Tier 2: reavaliação anual com questionário atualizado e verificação de certificações.

37

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		



- Tier 3 e 4: monitoramento conforme periodicidade definida na classificação.

São gatilhos de reavaliação imediata, independentemente do tier: incidente de segurança confirmado envolvendo o Terceiro; mudança de controle societário (fusão, aquisição); notícia pública de vazamento de dados ou sanção regulatória; subcontratação não autorizada de atividades no escopo do contrato; e degradação significativa de SLA sem justificativa técnica aceitável.

17.6 RESPOSTA A INCIDENTES COM VETOR EM TERCEIRO

Ao identificar ou receber notificação de incidente de segurança com origem ou impacto em Terceiro, o CISO ou o owner interno aciona imediatamente o playbook de resposta a incidentes com vetor em Terceiro, avaliando em até 2 horas:

- Escopo dos dados e sistemas potencialmente afetados.
- Necessidade de isolamento imediato dos acessos do Terceiro — realizado preventivamente sempre que houver evidência ou suspeita razoável de comprometimento, independentemente de confirmação formal do incidente.
- Necessidade de acionamento de um provedor alternativo.
- Obrigações de notificação regulatória.

A responsabilidade pelas obrigações regulatórias de notificação permanece com a Instituição como controladora dos dados e como instituição regulada, independentemente de o vetor ter sido um Terceiro. Os prazos de comunicação a ANPD (2 dias úteis — LGPD, Art. 48, e Resolução CD/ANPD no 15/2024) e ao BACEN (Resolução CMN no 4.893/2021, Art. 20, III) são contados a partir do momento em que a

38

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

Instituição toma ciência do incidente. O Terceiro é solidariamente responsável pelos danos decorrentes do descumprimento de suas obrigações contratuais de segurança, com direito de regresso da Instituição (LGPD, Art. 42).

17.7 CONCENTRAÇÃO DE RISCO E ESTRATÉGIA DE SAÍDA

A Instituição monitora ativamente o risco de concentração em fornecedores únicos para serviços críticos. Para cada Terceiro Tier 1 identificado como single point of failure, são documentados e mantidos atualizados: plano de saída formal (exit strategy) com procedimento detalhado de migração de dados e workloads, prazo estimado de transição e provedores alternativos previamente avaliados; e testes periódicos do plano de saída com frequência mínima anual para provedores de cloud críticos.

18. CONSCIENTIZAÇÃO E TREINAMENTO DE SEGURANÇA

A Instituição mantém programa contínuo e estruturado de conscientização e treinamento em segurança da informação, como mecanismo de disseminação da cultura de segurança cibernética..

O programa contempla:

- Treinamento obrigatório integrado ao processo de onboarding de todos os novos colaboradores.
- Treinamento anual de reciclagem para todos os colaboradores, com trilhas diferenciadas por perfil de risco e função.
- Simulações de phishing e outros vetores de engenharia social e testes práticos, como campanhas de phishing controlado

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

- Atualização contínua dos programas para refletir novas ameaças e regulamentações
- Monitoramento da eficácia dos treinamentos por meio de avaliações e métricas
- Prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros.

19. MONITORAMENTO, RELATÓRIO ANUAL E MELHORIA CONTÍNUA

O relatório operacional ao Comitê de Segurança da Informação e à Diretoria é apresentado com periodicidade mínima trimestral, e contempla: (i) incidentes relevantes e causa-raiz; (ii) resultado dos pentests e status do plano de ação; (iii) resultado dos testes de continuidade; (iv) vulnerabilidades abertas por criticidade e conformidade com os SLAs da Seção 12.1; (v) indicadores de CTI; e (vi) indicadores de conformidade regulatória. Registrado em ata e retido por no mínimo 5 anos.

A Instituição institui mecanismos formais de acompanhamento e controle para assegurar a implementação e a efetividade desta Política, do Plano de Resposta a Incidentes e dos requisitos de contratação de serviços em nuvem.

20. VIGÊNCIA DA POLÍTICA

Esta Política tem vigência de 01 (um) ano contado da sua aprovação, podendo ser revisada a qualquer momento sempre que forem identificados fatos que gerem impacto sobre as presentes disposições, incluindo alterações regulatórias, incidentes relevantes ou mudanças significativas no ambiente tecnológico ou de negócios da Instituição.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

21. HISTÓRICO DE ALTERAÇÕES

Data	Versão	Descrição	Responsáveis
12/06/2026	1.0	Aprovação	Marcelo Feitoza (Diretor Estatutário)
12/06/2026	1.0	Aprovação	Marcelo Almeida (Diretor Estatutário)
12/06/2026	1.0	Revisão e Aprovação	Daniel Freire (Diretor de Tecnologia - CTO)
10/06/2026	1.0	Revisão e Aprovação	Wellington Cunha (Gerente de Segurança da Informação)
10/06/2026	1.0	Revisão Geral	Sama Paes (Compliance)
10/06/2026	1.0	Criação do Documento	Luiz Claudio (Especialista Cyber)

22. REFERÊNCIAS NORMATIVAS

22.1. REGULAMENTAÇÃO

- Lei nº 13.709/2018 — Lei Geral de Proteção de Dados (LGPD).
- Lei nº 12.965/2014 — Marco Civil da Internet.
- Lei Complementar nº 105/2001 — Sigilo das operações de instituições financeiras.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

- Decreto nº 9.637/2018 — Política Nacional de Segurança da Informação (PNSI).
- Resolução CMN nº 4.893/2021 — Política de Segurança Cibernética para instituições financeiras.
- Resolução CMN nº 5.274/2025 — Atualiza e aprofunda os controles mínimos de segurança cibernética previstos na CMN nº 4.893/2021, com vigência a partir de 1º de março de 2026, aplicável a instituições autorizadas a funcionar pelo Banco Central.
- Resolução CD/ANPD nº 15/2024 — Notificação de incidentes de segurança com dados pessoais.

22.2. NORMAS TÉCNICAS

- ABNT NBR ISO/IEC 27001:2022 — Sistemas de Gestão da Segurança da Informação (SGSI).
- ABNT NBR ISO/IEC 27002:2022 — Controles de Segurança da Informação.
- ISO/IEC 27701:2019 — Sistema de Gestão de Privacidade da Informação.
- ISO/IEC 27017:2015 — Controles de segurança para Cloud Computing.
- ISO/IEC 27018:2019 — Proteção de dados pessoais em cloud.

22.3. Frameworks e Boas Práticas

- NIST Cybersecurity Framework (CSF) 2.0.
- NIST SP 800-61 Rev. 3 — Computer Security Incident Handling Guide (2024).
- NIST SP 800-88 Rev. 1 — Guidelines for Media Sanitization.
- NIST SP 800-207 — Zero Trust Architecture.
- NIST SP 800-161 Rev. 1 — Cybersecurity Supply Chain Risk Management.
- CIS Controls v8 — Center for Internet Security.
- OWASP API Security Top 10 (2023); OWASP ASVS v4.0; OWASP Top 10 CI/CD Security Risks (2022).
- MITRE ATT&CK Framework for Enterprise e Financial Services.

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		

- DOE Cybersecurity Capability Maturity Model (C2M2) v2.1.
- SANS Security Awareness Maturity Model.
- ANPD Guia Orientativo de Direitos dos Titulares (2023).
- NBR ISO/IEC 27001 de 11/2022: Sistemas de Gestão da Segurança da Informação
- NBR ISO/IEC 27002 de 10/2022: Tecnologia da Informação - Técnicas de Segurança - Código de Práticas para Gerenciamento da Segurança da Informação
- ISO/IEC 27701:2019 – Extensão da 27001 para Privacidade e Gestão de Dados Pessoais
- ISO/IEC 27017:2015 – Controles de Segurança para Cloud Computing
- ISO/IEC 27018:2019 – Proteção de Dados Pessoais em Cloudpc
- ISO/IEC 42001:2023 – Sistemas de Gestão de Inteligência Artificial
- CIS Controls v8 – Center for Internet Security
- NIST Cybersecurity Framework (NIST CSF)

Área responsável	Seg. da Informação	Classificação da Informação	Corporativo
Versão	1.0	Tipo do Documento	Política Interna
Data da aprovação	12/06/2026		