POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

POL-0401
DATA 27/02/2026

ideal

1 PROPÓSITO

Estabelecer, no mais alto nível, os princípios, fundamentos e expectativas estratégicas para a Segurança da Informação na organização, definindo a direção e a obrigatoriedade de todos os demais documentos, controles e práticas que compõem o Sistema de Gestão de Segurança da Informação (SGSI).
A PSI determina como a organização protege seus dados, sistemas, processos e serviços, abrangendo aspectos de confidencialidade, integridade, disponibilidade, privacidade, rastreabilidade e resiliência operacional, em conformidade com:

- Normativos regulatórios aplicáveis (RES BCB 85/2021, RES BCB 538/2025, RES CVM 35), que estabelecem controles mínimos, requisitos de proteção para ambientes críticos (RSFN/Pix/STR) e padrões de segurança cibernética;
- A Lei Geral de Proteção de Dados (LGPD) e demais legislações vigentes;
- As boas práticas internacionais baseadas na ISO/IEC 27001:2022 e ISO/IEC 27002:2022.

A PSI funciona como norma-mestra: orienta, direciona e exige que todas as áreas sigam os princípios de segurança, adotem controles adequados, implementem evidências, gerenciem riscos, atuem em conformidade regulatória e mantenham ambiente seguro para clientes, colaboradores e operações.

2 ESCOPO

Este documento se aplica, de forma ampla e mandatória, a todas as unidades organizacionais, colaboradores, prestadores de serviço, fornecedores, sistemas, processos, plataformas tecnológicas e fluxos de informação envolvidos nas operações da organização.

O escopo da PSI abrange:

- **Todos os ambientes tecnológicos** utilizados pela organização, incluindo infraestrutura on-premises, nuvem pública/privada (SaaS, PaaS, IaaS), ambientes híbridos e recursos terceirizados;
- **Todos os ativos de informação**, independentemente de formato, criticidade ou local de armazenamento (dados, documentos, registros, logs, sistemas, APIs, integrações, bases de dados, artefatos de desenvolvimento e pipelines CI/CD);
- **Todos os usuários**, incluindo colaboradores, estagiários, temporários, terceiros, desenvolvedores externos, fornecedores de tecnologia e operadores de serviços críticos;
- **Todos os dispositivos e meios de acesso**, como endpoints corporativos, dispositivos móveis autorizados, serviços remotos e identidades digitais;
- **Ambientes e integrações reguladas**, incluindo, quando aplicável, RSFN, Pix e STR, que exigem controles específicos de segurança cibernética, isolamento, proteção de chaves, autenticação forte e rastreabilidade reforçada;
- **Processos de negócio, operações críticas e serviços essenciais**, incluindo prestação de serviços a clientes, tratamento de dados pessoais, continuidade, resposta a incidentes, desenvolvimento de software e gestão de fornecedores.

Este escopo garante que a PSI cubra integralmente todas as superfícies de risco e pontos de exposição, funcionando como limite formal para o SGSI e para as demais políticas e controles derivados.

3 REFERÊNCIAS NORMATIVAS

- Resolução BCB nº 538/2025
- Resolução BCB nº 85/2021
- Lei Geral de Proteção de Dados (LGPD)
- Resolução CVM nº 35/2021
- ISO/IEC 27001:2022 e ISO/IEC 27002:2022
- Documentos Corporativos relacionados (POL0403, POL0405, MAN0402 etc.)

4 PRINCÍPOS DA SEGURANÇA DA INFORMAÇÃO

4.1 CONFIDENCIALIDADE

Garantir que o acesso às informações ocorra apenas por pessoas autorizadas. Inclui:

- need-to-know e segregação de funções;
- MFA e políticas de senhas;
- criptografia em trânsito e repouso (incluindo backups);
- gestão segura de chaves e certificados;
- controle de acesso físico e lógico;
- descarte seguro de equipamentos e documentos.

4.2 INTEGRIDADE

Preservar exatidão e completude das informações. Inclui:

- trilhas de auditoria completas e imutáveis;
- testes de restauração de backups;
- catálogo de sistemas e dispositivos com responsáveis definidos.

4.3 DISPONIBILIDADE

Garantir acesso às informações quando necessário. Inclui:

- plano de continuidade com testes anuais;
- monitoração de capacidade e saúde dos sistemas;
- testes de estresse periódicos;
- gestão de incidentes com registros, tratamento e lições aprendidas.

4.4 PRIVACIDADE E PROTEÇÃO DE DADOS (LGPD)

- tratamento ético e sigiloso dos dados;
- proibição de uso indevido ou compartilhamento não autorizado;
- termo de confidencialidade para colaboradores;
- classificação das informações conforme políticas internas.

4.5 CONSCIENTIZAÇÃO E CULTURA

- programa contínuo de treinamentos anuais e campanhas;
- simulações (ex.: phishing) e recertificação quando necessária;
- cláusulas de SI em contratos relevantes;
- orientação sobre uso aceitável dos recursos tecnológicos.

5 DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO

As diretrizes gerais a seguir se aplicam transversalmente a todos os processos, áreas, sistemas, serviços, terceiros e ambientes tecnológicos da organização. Elas complementam os princípios da Política de Segurança da Informação e orientam a implementação dos controles definidos nos domínios posteriores, conforme exigências do BCB 538, LGPD e ISO/IEC 27001/27002 e demais normas aplicáveis.
As diretrizes de segurança cibernética devem ser aplicadas em conjunto com a POL0403 – Política de Segurança Cibernética (PSC), que estabelece controles técnicos, requisitos de monitoramento, resposta a incidentes, barreiras de proteção, governança de nuvem e critérios de proteção contra ameaças cibernéticas.

5.1 PRÁTICAS FUNDAMENTAIS

- **Segurança por design e por padrão:** requisitos mínimos de Segurança da Informação e privacidade devem ser incorporados desde a concepção de processos, sistemas, integrações e fluxos de dados.
- **Menor privilégio e necessidade de saber:** acessos devem ser concedidos exclusivamente conforme necessidade funcional, com segregação de funções quando aplicável.
- **Rastreabilidade ponta a ponta:** toda ação relevante em ambiente produtivo deve gerar trilha de auditoria que permita identificar quem, quando, o que, onde e por que.
- **Criptografia obrigatória:** dados corporativos e de clientes devem ser protegidos em trânsito e repouso, incluindo cópias de segurança.
- **Proteção de dados pessoais:** tratamento conforme LGPD, incluindo minimização, base legal, controle de acesso e respostas a titulares.

5.2 REQUISITOS OPERACIONAIS TRANSVERSAIS

- **Retenção de evidências e registros:** logs, trilhas, relatórios, mensagens regulatórias e evidências devem ser mantidos pelo prazo mínimo de 5 anos, conforme exigências do BCB.

- **Monitoramento contínuo:** eventos de segurança, capacidade, integridade e desempenho dos sistemas devem ser monitorados de forma sistemática.
- **Gestão de vulnerabilidades:** identificação, avaliação e correção contínua de vulnerabilidades, incluindo pentests periódicos conforme criticidade.
- **Configuração segura:** ativos devem seguir padrões de hardening e controles mínimos exigidos pelas normas vigentes.
- **Segurança em integrações:** APIs e interfaces eletrônicas devem utilizar autenticação forte, escopos mínimos, rate-limit, proteção de segredos e validação de entrada.

5.3 TERCEIROS, NUVEM E FORNECEDORES

- **Due diligence obrigatória:** qualquer fornecedor, crítico ou não, deve ser avaliado previamente quanto a riscos, controles e conformidade.
- **Cláusulas contratuais de SI:** contratos devem incluir requisitos de segurança equivalentes aos internos, incluindo proteção de dados, auditoria, notificações e tratamento de incidentes.
- **Segurança em nuvem:** ambientes devem prever segregação adequada, gestão de chaves, restrição de acesso a credenciais e aderência aos controles mínimos do BCB.

5.4 COMPORTAMENTO E USO ACEITÁVEL

- **Uso adequado de recursos tecnológicos:** ferramentas corporativas (e-mail, endpoints, mensagens, infraestrutura) devem ser utilizadas exclusivamente para fins autorizados.
- **Proibição de compartilhamento não autorizado:** dados corporativos, pessoais ou confidenciais não podem ser acessados, utilizados ou compartilhados sem autorização.
- **Responsabilidade individual:** todos os usuários são responsáveis por proteger informações e reportar incidentes ou suspeitas imediatamente.

6 PAPÉIS E RESPONSABILIDADES

- **Diretoria**
  - Aprovar esta política e suas atualizações.
  - Patrocinar e promover a cultura de Segurança da Informação.
  - Assegurar cumprimento das obrigações regulatórias aplicáveis.

- **Segurança da Informação (SI)**
  - Manter esta política e o arcabouço documental do SGSI.
  - Definir diretrizes, requisitos e critérios mínimos de segurança.
  - Coordenar a resposta a incidentes e apoiar a conformidade regulatória.
  - Orientar TI e Áreas de Negócio na implementação de controles.

- **Tecnologia da Informação (TI)**
  - Implementar e operar controles técnicos definidos por SI.
  - Administrar infraestrutura, operações, monitoramento, registros de logs, patching e mudanças.
  - Proteger chaves, credenciais e componentes críticos.
  - Apoiar iniciativas de segurança e privacidade.

- **Áreas de Negócios**
  - Definir requisitos de uso, classificação e propósito dos dados sob sua responsabilidade.
  - Garantir que suas equipes cumpram as diretrizes de segurança da informação.
  - Validar acessos conforme necessidade funcional.

- **Risco**
  - Estabelecer diretrizes corporativas de gestão de risco.
  - Consolidar riscos de toda a organização para visão integrada.
  - Orientar priorizações conforme apetite de risco corporativo.

- **Compliance, Jurídico e DPO**
  - Monitorar aderência a requisitos legais e regulatórios.
  - Apoiar comunicações às autoridades e titulares, quando aplicável.
  - Orientar áreas operacionais sobre obrigações de privacidade e proteção de dados.

7 GESTÃO DE RISCOS

A organização adota gestão de riscos de Segurança da Informação como processo contínuo e essencial para preservar confidencialidade, integridade, disponibilidade, privacidade e rastreabilidade.

7.1 DIRETRIZ GERAL

A gestão de riscos deve seguir metodologia formal da área de Segurança da Informação, alinhada à ISO/IEC 27001/27005, BCB 538/2025 e LGPD, dentre outras normas aplicáveis, definindo critérios, processos e responsabilidades fora desta PSI.

7.2 PRINCÍPIOS

- Decisões baseadas em risco.
- Controles proporcionais ao impacto e à exposição.
- Revisão contínua conforme mudanças tecnológicas, regulatórias ou de negócio.

7.3 ESCOPO

O processo deve contemplar ativos de informação, ambientes internos e externos, terceiros, nuvem, projetos, mudanças relevantes e, quando aplicável, ambientes regulados RSFN/Pix/STR.

7.4 RESPONSABILIDADES

- **Segurança da Informação**
  - Manter metodologia, critérios e ferramentas de avaliação.
  - Identificar, registrar e consolidar riscos tecnológicos e de segurança.
  - Propor planos de tratamento alinhados às necessidades de negócio.
  - Escalonar riscos relevantes ao Time de Riscos Corporativos.

- **Risco**
  - Avaliar riscos recebidos de TI/SI sob perspectiva corporativa e de apetite de risco.
  - Consolidar riscos de diferentes áreas para visão integrada da organização.
  - Recomendar encaminhamento e necessidade de aprovação executiva.
  - Garantir aderência às políticas corporativas de risco.

- **Proprietários de sistemas/dados**
  - Identificar riscos inerentes ao uso, operação ou alteração de seus ativos.
  - Avaliar impactos de negócio e apoiar definição do tratamento.

- Executar e acompanhar os planos de tratamento sob sua responsabilidade.

- **Diretoria**
  - Aprovar riscos classificados como altos ou críticos.
  - Validar exceções, aceitar riscos residuais e orientar priorização estratégica.

- **Auditoria Interna**
  - Avaliar a eficácia, aderência e independência do processo de gestão de riscos.
  - Emitir recomendações com base na maturidade do SGSI e das práticas corporativas.

8 DIRETRIZES E CONTROLES POR DOMÍNIO

As diretrizes a seguir foram organizadas e estruturadas conforme os domínios da ISO/IEC 27002:2022, incorporando o mapeamento obrigatório para os 14 controles mínimos previstos nas resoluções BCB 538/2025. O mapeamento também considera o Art. 3º, §3º das normas, que estende a aplicação dos controles a novas tecnologias, desenvolvimento seguro e sistemas/serviços de terceiros.

8.1 CLASSIFICAÇÃO DA INFORMAÇÃO

Objetivo:

Estabelecer critérios consistentes para classificar e proteger informações conforme sensibilidade, valor e requisitos legais.

Diretrizes e Controles:

- Manter esquema de classificação que oriente manuseio, acesso e descarte conforme nível de sensibilidade (Cobertura: IV, IX, II).
- Reavaliar a classificação quando houver mudança de criticidade/finalidade (Cobertura: VI).

Documentos Corporativos com detalhamento:

- MAN0413 – Classificação da Informação

8.2 IDENTIDADES, MATRIZ DE SEGREGAÇÃO DE ACESOS, ACESSOS E PRIVILÉGIOS

Objetivo:

Garantir que o acesso a sistemas e informações seja autorizado, revisado e revogado conforme necessidade e requisitos regulatórios.

Diretrizes e Controles:

- Adotar processo formal de concessão, revisão e revogação de acessos, baseado em necessidade e segregação de funções (Cobertura: I, IX).
- Tratar acessos privilegiados com controles reforçados e trilhas completas (Cobertura: I, IX, VI).

Documentos Corporativos com detalhamento:

- MAN0402 – Concessão de Acessos

8.3 PRIVACIDADE E PROTEÇÃO DE DADOS

Objetivo

Assegurar o tratamento adequado de dados pessoais, preservando direitos dos titulares e conformidade com a legislação.

Diretrizes e Controles:

- Aplicar minimização, base legal e controles de segurança para dados pessoais (Cobertura: II, IV, IX, VI).

Documentos Corporativos com detalhamento:

- POL0512 - Política de Privacidade e Uso de Dados Pessoais
- POL0515 - Diretrizes para Tratamento e Uso de Dados Pessoais

8.4 CRIPTOGRAFIA E GESTÃO DE CHAVES

Objetivo:

Proteger informações em trânsito e repouso por meios criptográficos adequados.

Diretrizes e Controles:

- Definir e aplicar requisitos mínimos de criptografia e gestão de certificados (Cobertura: II, XII).
- Proteger chaves privadas durante todo o ciclo de vida com controles de acesso e auditoria (Cobertura: II, XII, IX, VI).

Documentos Corporativos com detalhamento:

- MAN0414 – Gerenciamento de Chaves Criptográficas

8.5 SEGURANÇA OPERACIONAL

Objetivo:

Promover a operação segura dos ambientes tecnológicos, garantindo controle, estabilidade e rastreabilidade.

Diretrizes e Controles:

- Implementar mecanismos formais de prevenção de vazamento de informações (DLP), incluindo monitoramento, alerta, restrição ou bloqueio de movimentação de dados conforme sua classificação (Cobertura: IV – Prevenção de Vazamento).**
- Conduzir gestão de mudanças formal e inventário/CMDB atualizados (Cobertura: VI).

- Coletar e reter logs relevantes em ambiente protegido (Cobertura: VI).
- Estabelecer processo de gestão de vulnerabilidades com prazos de correção e validações (Cobertura: VIII).
- Manter proteção antimalware em ativos pertinentes (Cobertura: V).
- Aplicar perfis de configuração segura (hardening) a ativos e plataformas (Cobertura: X).
- Realizar pentest independente anual e após mudanças relevantes (requisito reforçado pelo regulador).
- Os resultados dos testes de intrusão independentes (pentests) e das varreduras de vulnerabilidades, bem como seus respectivos planos de ação, devem compor o relatório anual de segurança requerido pelo regulador e ser mantidos por, no mínimo, 5 anos.

Documentos Corporativos com detalhamento:

- MAN0406 - Gestão de Mudanças
- POL0408 - Política de Gestão e Retenção de Logs
- MAN0415 - Cadastro de Aplicações no CMDB

8.6 SEGURANÇA DE REDES E ACESSO REMOTO

Objetivo:

Proteger a infraestrutura de rede e acessos remotos, reduzindo riscos de exposição e acesso indevido.

Diretrizes e Controles:

- Manter segmentação adequada entre ambientes e funções (Cobertura: XI).
- Exigir autenticação forte e canais protegidos para acesso remoto (Cobertura: I, II).
- Garantir segurança em integrações e interfaces eletrônicas (Cobertura: XIII).
- Adotar mecanismos de prevenção/detecção de intrusão e monitoramento contínuo, incorporando capacidade de Threat Intelligence (TI) para identificar, correlacionar e antecipar ameaças emergentes, incluindo monitoramento ativo de superfícies externas como internet, Deep Web e Dark Web, além de integrar práticas de DRP (Digital Risk Protection) para identificar, analisar e mitigar riscos cibernéticos externos relacionados a vazamentos, exposição indevida de dados, falsos domínios, credenciais comprometidas e atividades maliciosas vinculadas à instituição (Cobertura: III, XI, VI).

Documentos Corporativos com detalhamento:

- MAN0412 - Acesso Remoto à Infraestrutura
- MAN0414 - Gerenciamento de Chaves Criptográficas
- POL0408 - Política de Gestão e Retenção de Logs
- MAN0406 - Gestão de Mudanças

8.7 CONTINUIDADE, RESILIÊNCIA E BACKUP

Objetivo:

Assegurar que operações críticas possam ser mantidas ou restabelecidas dentro de prazos aceitáveis.

Diretrizes e Controles:

- Definir RTO/RPO e estratégias de recuperação para serviços críticos (Cobertura: VI).
- Manter políticas de backup com testes periódicos de restauração (Cobertura: VII).

Documentos Corporativos com detalhamento:

- POL0405 - Gestão de Continuidade de Negócios
- POL0402 - Concessão de Acessos

8.8 DESENVOLVIMENTO SEGURO (SDLC, APIS E INTEGRAÇÕES)

Objetivo:

Promover práticas de desenvolvimento seguro, garantindo que sistemas e integrações sigam requisitos de segurança e privacidade.

Diretrizes e Controles:

- Incluir requisitos de segurança desde a concepção e aplicar controles também em novas tecnologias e sistemas de terceiros (Cobertura: §3 – desenvolvimento seguro/novas tecnologias/terceiros; I, II, IX, XIII).
- Estabelecer revisões e verificações de segurança no SDLC, com rastreabilidade de mudanças (Cobertura: VI, VIII, XIII).
- Realizar implantação por fluxos controlados e auditáveis (Cobertura: VI).

Documentos Corporativos com detalhamento:

- POL0407 – Desenvolvimento Seguro

8.9 FORNECEDORES E NUVEM

Objetivo:

Garantir que fornecedores e serviços em nuvem atendam aos requisitos de segurança, privacidade e continuidade estabelecidos pela organização.

Diretrizes e Controles:

- Avaliar riscos e conformidade antes da contratação, exigindo aderência aos 14 controles mínimos quando aplicável (Cobertura: I–XIV, §3 – terceiros).
- Incluir, em contrato, requisitos mínimos de segurança e notificação de incidentes (Cobertura: VI, VIII, XIII).
- Observar segregação, controle de acesso e proteção de dados equivalentes aos ambientes internos (Cobertura: II, IX, XI).

Documentos Corporativos com detalhamento:

- POL0403 - Política de Segurança Cibernética

8.10 GESTÃO DE INCIDENTES E REPORTES

Objetivo:

Estabelecer capacidade estruturada para identificação, resposta, comunicação e reporte de incidentes de segurança.

Diretrizes e Controles:

- Manter processo formal de gestão de incidentes, com análise, documentação, ações corretivas e reporte quando aplicável (Cobertura: VI, VIII).
- Utilizar lições aprendidas para melhoria contínua (Cobertura: VI).

Documentos Corporativos com detalhamento:

- MAN0405 - Gestão de Incidentes

8.11 CAPACIDADE E DESEMPENHO

Objetivo:

Garantir que recursos tecnológicos atendam aos níveis de desempenho e disponibilidade necessários às operações.

Diretrizes e Controles:

- Monitorar desempenho e capacidade de forma contínua, com métricas e alertas definidos (Cobertura: VI – suporte à rastreabilidade operacional).
- Planejar expansão de capacidade com base em análise fundamentada (Cobertura: VI).
- As diretrizes específicas de gestão de capacidade, incluindo planejamento, monitoramento, indicadores-chave, incidentes e relatório executivo, devem seguir a POL0404 – Gestão de Capacidade.

Documentos Corporativos com detalhamento:

- POL0404 - Gestão de Capacidade

8.12 REQUISITOS ESPECÍFICOS - RSFN / PIX / STR

Objetivo:

Atender às exigências reforçadas para comunicação eletrônica de dados na RSFN, especialmente nos ambientes Pix e STR. Além disso, conforme orientação regulatória, a comunicação eletrônica via RSFN deve ser considerada serviço relevante, exigindo que quaisquer terceiros que participem dessa cadeia sejam formalmente classificados como fornecedores relevantes.

Diretrizes e Controles:

- Exigir MFA para acessos administrativos a ambientes Pix/STR (Cobertura: I).
- Manter isolamento físico e lógico dos ambientes Pix/STR dos demais sistemas; em nuvem, operar em instâncias dedicadas e apartadas (Cobertura: XI).
- Vedação de acesso de terceiros às chaves privadas da instituição utilizadas em SPI/Pix; supervisionar credenciais e certificados (Cobertura: XII, IX).
- Implementar validação de integridade fim a fim antes da assinatura digital das mensagens (Cobertura: II, VI, XII).
- Tratar comunicação eletrônica RSFN como serviço relevante para fins de contratação e gestão de riscos (Cobertura: I–XIV, §3 – terceiros).

9 CONSCIENTIZAÇÃO, TREINAMENTO E CULTURA

A organização manterá um Programa de Conscientização, Treinamento e Cultura de Segurança da Informação, alinhado às exigências regulatórias aplicáveis e às melhores práticas internacionais.

9.1 DIRETRIZES

- Todos os colaboradores, estagiários e terceiros e devem participar das ações obrigatórias de conscientização e treinamento.
- Os conteúdos devem abordar princípios de segurança da informação, privacidade, riscos humanos e responsabilidades individuais.
- O programa deve promover cultura contínua de segurança, com comunicações recorrentes e ações educativas proporcionais ao risco e ao perfil do público.
- Casos de comportamento inseguro recorrente podem exigir ações corretivas, incluindo reforço de treinamento.

9.2 RESPONSABILIDADES

- Segurança da Informação: estabelecer diretrizes do programa e garantir sua execução.
- Gestores: assegurar participação de suas equipes nos treinamentos obrigatórios.
- Usuários: cumprir os treinamentos e aplicar práticas seguras no dia a dia.

10 CONFORMIDADE, AUDITORIA E EVIDÊNCIAS

A organização deve manter processo contínuo de conformidade, garantindo aderência às políticas internas, legislações aplicáveis e exigências regulatórias (BCB 538/2025 e LGPD, dentre outras normas aplicáveis).

- Auditorias internas e externas devem ser realizadas periodicamente para verificar a eficácia dos controles de Segurança da Informação e identificar desvios.
- Evidências de conformidade como logs, relatórios, trilhas de auditoria, revisões de acesso, registros de mudanças, pentests e backups devem ser armazenadas em repositório seguro pelo prazo mínimo de 5 anos.

- Não conformidades devem gerar planos de ação formais, com prazos definidos, responsáveis claros e validação pela Segurança da Informação.
- A organização deve estar preparada para atender prontamente solicitações de reguladores, fornecendo informações e evidências de forma tempestiva, íntegra e rastreável.

11 EXCEÇÕES, ACEITE DE RISCO E DESVIOS

A adoção de qualquer prática, configuração, processo ou solução tecnológica que esteja fora dos requisitos definidos nesta PSI, em políticas complementares ou em controles obrigatórios, somente é permitida mediante processo formal de exceção.

11.1 EXCEÇÕES

- Devem ser solicitadas antes da implementação da medida excepcional.
- O pedido deve conter justificativa, impacto, mitigadores, prazo e responsável.
- A aprovação é responsabilidade da Segurança da Informação (SI) e, quando aplicável, de instância de governança equivalente ou superior.
- Exceções são temporárias, com prazo máximo definido e reavaliação obrigatória.

11.2 ACEITE DE RISCO

- Quando não houver mitigação adequada ou possível, pode ser adotado aceite de risco, formalizado conforme metodologia corporativa.
- Aceites devem ser aprovados conforme nível de risco, incluindo Diretoria para riscos altos ou críticos.
- Todo aceite de risco deve ser registrado no Risk Register Corporativo.

11.3 DESVIOS

- Descumprimentos involuntários das políticas, normas ou controles devem ser registrados como desvio.
- Desvios exigem análise de causa, mitigação e plano de ação com prazos definidos.
- Recorrência de desvios pode gerar ações disciplinares ou revisão de processos.

11.4 REGISTRO E EVIDÊNCIAS

- Todos os pedidos, aprovações, rejeições, revisões e encerramentos devem ser registrados e mantidos pelo prazo mínimo de 5 anos, conforme exigências regulatórias.

12 CONSEQUÊNCIAS PELO DESCUMPRIMENTO

O descumprimento das diretrizes, controles e obrigações estabelecidas nesta Política e em seus documentos complementares pode resultar em medidas disciplinares, administrativas e técnicas, proporcionais à gravidade da infração e ao nível de risco gerado para a organização.

12.1 Medidas Disciplinares e Administrativas

Podem incluir, conforme normas internas e legislação aplicável:

- advertência verbal ou escrita;
- suspensão de acesso a sistemas, dados ou recursos tecnológicos;
- suspensão temporária das atividades;
- desligamento, nos casos de maior gravidade ou reincidência.

12.2 Medidas Técnicas

A equipe de Segurança da Informação poderá adotar medidas imediatas para contenção de riscos, como:

- bloqueio ou revogação de credenciais;
- isolamento de dispositivos ou serviços;
- restrição temporária de funcionalidades;
- exigência de reciclagem ou reforço de treinamento.

12.3 Desvios Críticos ou Intencionais

Infrações que envolvam dolo, fraude, violação intencional de controles, tentativa de burlar mecanismos de segurança, vazamento de dados ou comprometimento de ambientes críticos (inclusive RSFN/Pix/STR, quando aplicável) serão tratadas com rígida resposta disciplinar, podendo incluir desligamento por justa causa.

12.4 Responsabilidades Legais e Civis

Quando o descumprimento representar violação à LGPD, regulamentação do Banco Central, contratos, sigilo profissional ou outras obrigações legais, a organização poderá:

- reportar o incidente às autoridades competentes;
- aplicar medidas administrativas, civis ou criminais cabíveis;
- responsabilizar contratualmente colaboradores, fornecedores ou terceiros.

12.5 Terceiros e Fornecedores

Para fornecedores, PSTIs e terceiros, o descumprimento das obrigações contratuais de Segurança da Informação poderá resultar em:

- multas contratuais;
- suspensão ou encerramento do contrato;
- restrição de uso futuro da empresa como fornecedor;
- reporte a áreas regulatórias, quando aplicável.

13 CICLO DE VIDA, REVISÃO E VIGÊNCIA

O Ciclo de Vida desta política estabelece seu processo de criação, manutenção, revisão e vigência, assegurando alinhamento constante às regulamentações e às necessidades do negócio.

13.1 Publicação e Vigência

- Esta PSI entra em vigor imediatamente após sua aprovação pela Diretoria.
- A publicação deve ocorrer em repositório corporativo oficial, acessível a todos os colaboradores e terceiros relevantes.

13.2 Revisão Periódica

- A PSI deve ser revisada anualmente, ou em prazo menor quando houver:
  - mudanças regulatórias;
  - mudanças tecnológicas relevantes;
  - alteração significativa de processos, riscos ou estrutura organizacional;
  - eventos críticos de segurança que indiquem necessidade de atualização.
- Toda revisão deve ser conduzida pela área de Segurança da Informação, com participação das áreas impactadas.

13.3 Aprovação e Governança

- Revisões ou atualizações só entram em vigor após aprovação formal da Diretoria.
- Mudanças estruturais ou de impacto regulatório devem ser previamente avaliadas por Segurança da Informação, Compliance e Jurídico.

13.4 Controle de Versões e Evidências

- Todas as versões da PSI devem possuir histórico documentado contendo data, responsável pela atualização, resumo de alterações e aprovação.
- Evidências de revisão, aprovação e publicação devem ser mantidas em repositório seguro pelo prazo mínimo de 5 anos.

13.5 Descontinuidade

- Uma versão só pode ser substituída após publicação da nova versão aprovada; versões antigas devem ser arquivadas e marcadas como Revogado.

14 TERMOS E DEFINIÇÕES

Para garantir clareza, padronização e evitar interpretações divergentes, esta seção consolida os principais termos utilizados nesta PSI e nos documentos que a complementam.

14.1 TERMOS GERAIS DE SEGURANÇA DA INFORMAÇÃO

- **Ameaça:** causa potencial de um incidente indesejado.
- **Ativo de informação:** qualquer dado, sistema, pessoa, processo, infraestrutura, serviço ou componente tecnológico que possua valor para a organização.
- **Confidencialidade:** garantia de que a informação é acessada apenas por pessoas autorizadas.
- **Controles:** medidas técnicas, administrativas ou físicas aplicadas para mitigar riscos.
- **Disponibilidade:** garantia de acesso às informações e recursos quando necessário.
- **Evento de Segurança:** ocorrência identificada que pode ser relevante para monitoramento, mas não necessariamente configura incidente.
- **Incidente de Segurança da Informação:** evento que possa comprometer confidencialidade, integridade, disponibilidade, privacidade ou resiliência.
- **Integridade:** proteção contra modificação não autorizada ou acidental.
- **Rastreabilidade / Auditabilidade:** capacidade de identificar quem executou determinada ação, quando, onde e como.
- **Risco:** combinação entre a probabilidade de exploração de uma vulnerabilidade e o impacto resultante.
- **Vulnerabilidade:** fraqueza que pode ser explorada por uma ameaça.

14.2 TERMOS RELACIONADOS A IDENTIDADES, ACESSOS E USUÁRIOS

- **Base legal:** fundamento jurídico para o tratamento de dados pessoais.
- **Credencial:** informação utilizada para autenticação (ex.: senha, token, certificado).
- **Controlador:** quem toma decisões sobre o tratamento de dados.
- **Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável.
- **Dado pessoal sensível:** dado que exige maior proteção, como biometria, saúde, crença, origem, entre outros.
- **Encarregado (DPO):** responsável pela comunicação entre controlador, titulares e ANPD.
- **IGA (Identity Governance and Administration):** governança sobre o ciclo de vida das identidades e acessos.
- **MFA (Autenticação Multifator):** combinação de dois ou mais fatores (conhecimento, posse, biometria).
- **Operador:** quem processa dados conforme instruções do controlador.

- **PAM (Privileged Access Management):** conjunto de controles para gerenciar e proteger acessos privilegiados.
- **Privilégio / Acesso privilegiado:** permissão que concede capacidade elevada de alteração, administração ou consulta sensível.
- **Titular:** pessoa natural a quem se referem os dados pessoais.
- **Usuário:** qualquer pessoa que utilize recursos tecnológicos corporativos.

14.3 TERMOS RELACIONADOS A TECNOLOGIA, NUVEM E INTEGRAÇÕES

- **Ambiente em nuvem:** infraestrutura ou plataforma computacional sob responsabilidade de provedores externos.
- **API (Application Programming Interface):** interface de comunicação entre sistemas.
- **Integração:** fluxo de troca de dados entre sistemas internos ou externos.
- **CI/CD:** conjunto de práticas e ferramentas para integração e entrega contínuas.
- **Hardening:** aplicação de padrões de configuração segura.
- **DLP (Data Loss Prevention):** tecnologia para prevenir vazamentos de dados.

14.4 TERMOS RELACIONADOS À SEGURANÇA CIBERNÉTICA

- **Ambiente crítico:** ambientes sujeitos a controles reforçados conforme regulamentações do Banco Central.
- **Certificados digitais:** mecanismos criptográficos usados para autenticação e assinatura.
- **Isolamento lógico/físico:** separação entre ambientes para evitar interferências ou acesso indevido.
- **Pentest:** teste de intrusão autorizado para avaliar segurança.
- **Detecção de intrusão (IDS/IPS):** mecanismos para identificar e bloquear ataques.

14.5 TERMOS RELACIONADOS A TERCEIROS E FORNECEDORES

- **Fornecedor crítico:** fornecedor cujo serviço impacta diretamente segurança, continuidade ou regulamentação.
- **PSTI (Prestador de Serviços de Tecnologia da Informação):** fornecedor de tecnologia sujeito a requisitos regulatórios.
- **Due diligence:** avaliação prévia de riscos antes de contratação.
- **SLA:** acordo de nível de serviço.

15 HISTÓRICO DE REVISÕES

Revisor	Data	Descrição
Fabio Farias	01/11/2018	Versão inicial
Fabio Farias	26/06/2019	Inclusão do capítulo de “Segurança no descarte de material impresso” Inclusão do capítulo de “Segurança no descarte de mídias físicas e equipamentos de TI”
Fabio Farias	29/10/2019	Revisão Anual Inclusão do capítulo “Escaneamento de Vulnerabilidades” Alteração na Política de Senhas Alteração no Uso de Internet Alteração nos Acessos Lógicos
Peter Klein	31/10/2019	Ajustes periféricos e revisão das inclusões.
Diretoria	05/11/2019	Aprovação versão 2.0
Fabio Farias	29/07/2020	Incorporação das diretivas da política de segurança cibernética e sistematização de uma gestão integrada das disciplinas. Reorganização geral dos assuntos e adaptações à luz da ICVM 612. Alteração no leiaute do documento em adequação ao novo sistema visual da marca
Peter Klein	11/08/2020	Revisão das alterações promovidas por TI
Diretoria	31/08/2020	Aprovação versão 3.0
Fabio Farias	04/12/2020	Adição de critérios para contratação de serviços em nuvem
Lucas Cury	09/12/2020	Detalhamento e diferenciação entre critérios de decisão e requisitos de contratação de serviços em nuvem.
Márcio Ramalho	26/10/2021	Revisão Anual 2021
Peter Klein	25/11/2021	Revisão das alterações promovidas por TI – versão 6.0
Diretoria	01/12/2021	Aprovação versão 6.0
Thais Devides	06/07/2022	Revisão do formato da Política e reorganização das diretrizes. A partir desta versão passou a se tratar a matéria de SI de forma independente retomando a sua contagem a partir da versão 3.0 em linha com o banco de Políticas da Corretora.
Diretoria	16/05/2023	Aprovação da versão 3.0 da POL0401 – Segurança da Informação (desmembrada).
Ricardo Lima	05/05/2025	Revisão Periódica 2025 (versão 4) e atualização das normativas que regem o documento.
Ricardo Lima	27/02/2026	Revisão integral da PSI, com adequação à estrutura da ISO 27001, incluindo reorganização por domínios conforme o framework, e atualização geral para alinhamento às exigências do BCB.

16 ANEXO A - MAPA DE COBERTURA BCB 538/2025

A tabela abaixo apresenta o mapeamento explícito entre os 14 controles mínimos obrigatórios definidos na resolução BCB 538/2025 e as respectivas seções/diretrizes da PSI onde cada controle é atendido.

16.1 MAPA DE COBERTURA DOS CONTROLES MÍNIMOS

Controle Obrigatório (BCB/CMN)	Seção / Domínio
I - Autenticação	9.2, 9.6, 9.12
II - Criptografia	9.1, 9.3, 9.4, 9.6, 9.12
III - Detecção de Intrusão (IDS/IPS)	9.6
IV - Prevenção de Vazamento (DLP)	9.1, 9.3, 9.5
V - Antimalware	9.5
VI - Rastreabilidade	9.1 - 9.12
VII - Backups	9.7
VIII - Vulnerabilidades	9.5, 9.8
IX - Controles de Acesso	9.1, 9.2, 9.4, 9.9, 9.12
X - Hardening / Configuração Segura	9.5
XI - Proteção de Rede	9.6, 9.12
XII - Certificados Digitais	9.4, 9.12
XIII - Integrações Seguras / APIs	9.6, 9.8, 9.9
XIV - Inteligência Cibernética	9.6

16.2 MAPA DE CONTROLES APLICÁVEIS A TERCEIROS E NUVEM

Controle Obrigatório (BCB/CMN)	Seção / Domínio
Controles mínimos aplicados a terceiros	9.9
Contratos com requisitos de SI	9.9
Segurança em nuvem equivalente ao ambiente interno	9.9
Sistemas de terceiros sujeitos ao SDLC seguro	9.8

16.3 MAPA RSFN/PIX/STR - EXIGÊNCIAS ESPECÍFICAS

Controle Obrigatório (BCB/CMN)	Seção / Domínio
MFA para acessos administrativos	9.12
Isolamento físico/lógico dos ambientes	9.12
Instâncias dedicadas na nuvem	9.12
Proibição de acesso de terceiros às chaves privadas	9.12
Validação de integridade ponta a ponta	9.12
Comunicação RSFN como serviço relevante	9.12