# Política de Segurança Cibernética

# Controle Do Documento

## Histórico de Revisão

| Versão | Data de Revisão | Autor da Revisão | Sumário de Mudanças |
|---|---|---|---|
| 1.0 | Outubro de 2022 | Lucas Nascimento | Versão inicial |
| 1.1 | Abril de 2024 | Lucas Nascimento | Revisão anual e textual |
| 2.0 | Janeiro de 2026 | Vanessa dos Santos Gallo | Atualização anual e alinhamento com a regulamentação vigente. |
| 2.1 | Março de 2026 | Vanessa dos Santos Gallo | Alinhamento com às Resoluções BCB nº 538 e nº 520. |

# Introdução

A **Nvio Brasil Bitso Instituição de Pagamento Ltda**., também denominada “Bitso do Brasil”, líder do Conglomerado Prudencial Nvio, atua como Instituição de Pagamento e integra, juntamente com a **Bitso Sociedade Prestadora de Serviços de Ativos Virtuais Ltda**. e outras entidades do grupo Bitso no Brasil, o conjunto de empresas que desenvolvem atividades relacionadas a arranjos e serviços de pagamento e, quando aplicável, à prestação de serviços envolvendo ativos virtuais.

Considerando que a Bitso Brasil é uma instituição regulada pelo Banco Central do Brasil, a Companhia deve cumprir as obrigações legais e regulatórias aplicáveis, incluindo aquelas relacionadas à Segurança da Informação, Cibersegurança e Proteção de Dados, mantendo políticas, procedimentos e controles compatíveis com a natureza de suas atividades e com os riscos a que está exposta.

## Objetivo

Esta Política de Segurança da Informação estabelece os princípios, diretrizes e responsabilidades para a proteção dos ativos de informação das entidades que compõem o conglomerado da Bitso no Brasil.

O documento tem como objetivo orientar a adoção de controles e práticas destinadas a assegurar a confidencialidade, integridade e disponibilidade das informações e dos sistemas utilizados pelas entidades do grupo, observando as disposições legais e regulatórias aplicáveis, bem como as melhores práticas de segurança da informação.

A política considera as atividades desempenhadas pelo grupo no país, incluindo aquelas sujeitas à supervisão do Banco Central do Brasil, **bem como aquelas relacionadas à prestação de serviços envolvendo ativos virtuais,** quando aplicável às entidades do conglomerado.

Nesse contexto, esta política busca:

- **Fortalecimento:** proteger informações e sistemas contra acessos indevidos, alterações não autorizadas e vazamentos de dados.
- **Continuidade:** assegurar que processos críticos permaneçam operacionais mesmo diante de incidentes, garantindo confiabilidade e disponibilidade.
- **Prevenção e mitigação:** prevenir, identificar, responder e reduzir vulnerabilidades e incidentes cibernéticos por meio de controles proativos e monitoramento contínuo.

- **Conformidade:** atender a todas as leis, regulamentos e normas aplicáveis, reforçando a governança e a responsabilidade legal.
- **Gestão de riscos:** Implementar práticas estruturadas de gestão de riscos cibernéticos, promovendo análise contínua de ameaças e aprimoramento constante das defesas digitais.

## Escopo

A Política deve ser observada e seguida por todos os colaboradores, consultores, prestadores de serviços, contratados, estagiários, fornecedores, parceiros de negócios e terceiros que atuem em nome da Bitso do Brasil ou que tenham acesso aos ativos de informação da Bitso do Brasil, incluindo sistemas, dados, redes e demais recursos tecnológicos.

## 1. Política de Segurança Cibernética

### 1.1. Diretrizes Gerais de Segurança da Informação

As diretrizes gerais têm como objetivo estabelecer os princípios fundamentais que orientam a gestão da segurança da informação na Companhia, servindo como base para todas as políticas, processos e procedimentos específicos subsequentes. Elas fornecem uma visão ampla sobre a proteção dos ativos de informação e definem o comportamento esperado de colaboradores, parceiros e terceiros, contemplando:

- **Confidencialidade, integridade e disponibilidade:** Garantir que as informações sejam acessadas apenas por pessoas autorizadas, permaneçam precisas e completas, e estejam disponíveis quando necessário;
- **Controles de segurança adequados:** Implementar mecanismos para prevenir acessos não autorizados, perdas, vazamentos e incidentes de segurança;
- **Conscientização contínua:** Promover a educação e o engajamento de todos na organização em relação às melhores práticas de segurança da informação;

- **Defesa em profundidade:** Adotar múltiplas camadas de proteção, de modo a reduzir riscos e fortalecer a resiliência contra ameaças;
- **Princípio do menor privilégio:** Garantir que o acesso às informações seja limitado apenas ao necessário para o desempenho das atividades;
- **Conformidade legal e regulatória:** Assegurar que todas as ações estejam alinhadas à legislação aplicável, regulamentações e políticas internas, sendo assim, observa-se que a Bitso do Brasil:
    - Mantém um nível aceitável de tolerância ao risco que equilibra de forma eficaz a produtividade do negócio, sem comprometer a confidencialidade, integridade ou disponibilidade da sua infraestrutura, produtos e serviços.

Essas diretrizes gerais estabelecerão a base estratégica e cultural da segurança da informação na Companhia, orientando a implementação de medidas concretas e específicas para proteger os ativos de informação e mitigar riscos.

# 2. Diretrizes Específicas de Segurança da Informação

As Diretrizes Específicas detalham e operacionalizam os princípios estabelecidos nas Diretrizes Gerais, definindo práticas obrigatórias para proteção, uso e compartilhamento seguro dos ativos de informação.

## 2.1.Gestão de Riscos Cibernéticos

A Companhia mantém um processo contínuo e integrado de gestão de riscos cibernéticos, alinhado à estrutura de Gerenciamento de Riscos Corporativos e às normas aplicáveis. A finalidade é identificar, avaliar e tratar ameaças que possam comprometer a confidencialidade, integridade e disponibilidade das informações.

## 2.2. Classificação das Informações

A Bitso do Brasil estabelece que todos os ativos de informação sejam formalmente classificados de acordo com sua sensibilidade, valor e criticidade, com base em critérios definidos nesta Política. O objetivo é assegurar a Confidencialidade, Integridade e Disponibilidade (CID) das informações e garantir a conformidade com as exigências legais e regulatórias aplicáveis.

## 2.3. Controle de Acesso

O controle de acesso é um dos pilares da **defesa em profundidade** da Bitso do Brasil, garantindo que apenas usuários devidamente autorizados tenham acesso a sistemas, informações e ambientes, de acordo com suas funções e responsabilidades.

As permissões de acesso devem ser revisadas periodicamente, incluindo aquelas concedidas a prestadores de serviço e colaboradores terceirizados que possuam acesso a recursos computacionais da Companhia, garantindo que tais acessos permaneçam compatíveis com suas funções e responsabilidades.

### 2.3.1. Gestão de Usuários

A gestão de acessos deve abranger todo o ciclo de vida do usuário criação, alteração, revisão e revogação e ser realizada conforme procedimentos específicos. Atribuições de acesso administrativo devem ser justificadas e documentadas, e sujeitas a revisão periódica pelo responsável. Contas de usuário inativas ou desnecessárias devem ser desativadas de acordo com o procedimento de Gestão de Acessos.

### 2.3.2. Autenticação e Política de Senhas

A autenticação deve assegurar a proteção das identidades e a integridade das contas de acesso aos sistemas e aplicações da Bitso do Brasil. Para tal:

- Autenticação multifator (MFA) é recomendada para todos os sistemas que a suportam e obrigatória para sistemas e dados classificados como críticos;

- Sempre que possível, deve-se adotar Single Sign-On (SSO) e mecanismos de autenticação federada, tokens ou certificados digitais;
- Recomenda-se o uso de tokens, certificados digitais ou autenticação federada sempre que aplicável;
- O compartilhamento de credenciais é proibido;
- Senhas devem obedecer aos critérios de complexidade definidos pela área de Segurança, conforme exposto abaixo:

| Critério | Descrição / Requisito |
|---|---|
| Comprimento mínimo | A senha deve conter no mínimo 15 caracteres. |
| Composição obrigatória | Deve incluir pelo menos uma letra maiúscula, uma letra minúscula e um símbolo especial. |
| Reutilização de senhas | É proibida a reutilização de senhas já utilizadas. Cada conta deve possuir uma senha única e exclusiva. |
| Frequência de mudança | Recomenda-se a alteração de senhas a cada 180 dias, ou sempre que houver suspeita de exposição. |
| Bloqueio de conta | A conta será bloqueada após cinco tentativas consecutivas de autenticação mal sucedidas. |

| | |
|---|---|
| Desbloqueio da conta | O desbloqueio deve ser realizado pela Central de Serviços de TI, mediante a verificação da identidade do usuário. |
| Armazenamento de Senhas | As senhas devem ser geradas e armazenadas de forma segura, preferencialmente por meio de ferramentas de gerenciamento de senha aprovadas pela Bitso do Brasil . |

## 2.4. Trabalho Remoto

A Bitso do Brasil permite o regime de trabalho remoto, adotando medidas para proteger informações e ativos fora das dependências corporativas. O acesso remoto deve ser realizado preferencialmente em equipamentos corporativos ou, quando autorizado, em dispositivos pessoais (BYOD) que atendam aos requisitos de segurança definidos pela área de Segurança da Informação.

Todos os equipamentos utilizados para acesso remoto devem seguir as diretrizes de segurança corporativas e ser devolvidos à Companhia em caso de desligamento.

## 2.5. Medidas de Prevenção, Detecção e Resposta a Incidentes

A Bitso do Brasil adota medidas técnicas, administrativas e organizacionais voltadas à prevenção, detecção e resposta a incidentes de segurança da informação, com o objetivo de proteger a confidencialidade, integridade e disponibilidade dos ativos de informação, bem como mitigar impactos sobre processos, pessoas e sistemas críticos, em conformidade com as exigências legais e regulatórias, incluindo a Resoluções do Banco Central do Brasil.

### 2.5.1. Prevenção

Para reduzir a probabilidade de incidentes, devem ser implementados controles preventivos que garantam a proteção da infraestrutura, conforme exemplificado a seguir (rol não taxativo):

- **Firewall:** Deve ser instalado em todos os pontos de conexão da rede interna com a Internet. Sempre que possível, os firewalls locais também devem ser ativados nos equipamentos dos usuários. As permissões de acesso devem impedir que o usuário desative o firewall;
- **Ferramentas anti-malware:** Todos os dispositivos devem possuir plataforma anti-malware corporativa com varredura em tempo real, configurada e gerenciada centralmente para evitar alterações pelos usuários. A solução deve manter-se atualizada e gerar logs de auditoria;
- **Ferramenta de Detecção de Intrusão:** A companhia mantém implementadas soluções de monitoramento e defesa, como sistemas de detecção e prevenção de intrusões (IDS/IPS), com o objetivo de identificar, alertar e mitigar possíveis ameaças à infraestrutura tecnológica;
- **Filtro de spam:** E-mails não solicitados e anexos potencialmente maliciosos devem ser filtrados antes de chegarem aos usuários. Tipos de arquivos conhecidos por conter malware devem ser bloqueados;
- **Prevenção de Vazamento de Informações (DLP):** Devem ser implementados controles para monitorar e impedir a transferência não autorizada de dados sensíveis e sigilosos para ambientes externos, dispositivos não seguros ou canais não aprovados;
- **Detecção em sandbox:** Sempre que aplicável, tecnologias de sandbox devem ser utilizadas para isolar e analisar executáveis suspeitos em ambiente controlado antes de permitir sua execução em ambiente produtivo;
- **Controle de instalação de software:** Usuários não devem possuir privilégios administrativos em seus dispositivos. Apenas softwares aprovados e licenciados podem ser instalados. Varreduras regulares devem ser realizadas para identificar e remover softwares não autorizados;

- **Gestão de vulnerabilidades:** Vulnerabilidades conhecidas devem ser monitoradas e corrigidas por meio da aplicação tempestiva de atualizações e patches. Varreduras regulares devem ser conduzidas, com prioridade para servidores e redes críticas ao negócio;
- **Conscientização e treinamento:** Todos os colaboradores devem participar de treinamentos de segurança da informação e campanhas de conscientização, incluindo exercícios simulados de phishing realizados, no mínimo, trimestralmente.

### 2.5.2. Detecção

A detecção de incidentes é contínua e apoiada por sistemas automatizados de monitoramento e alerta, incluindo soluções como EDR e SIEM, permitindo identificar rapidamente atividades suspeitas ou anômalas. Logs e eventos críticos devem ser coletados, analisados e correlacionados por essas ferramentas, garantindo visibilidade e fundamentação para a resposta a incidentes.

### 2.5.3. Resposta a Incidentes

Sempre que for detectada uma ameaça, vulnerabilidade explorada, falha de segurança, presença de malware ou qualquer outro evento que possa comprometer a confidencialidade, integridade ou disponibilidade das informações, deverá ser formalmente registrado um Incidente de Segurança da Informação.

## 2.6. Controles Técnicos Específicos

Além das medidas de prevenção, detecção e resposta a incidentes, a Companhia adota controles técnicos específicos para reforçar a segurança dos ativos de informação, garantir a continuidade das operações e reduzir riscos de comprometimento.

## 2.7. Registro e Monitoramento

A Bitso do Brasil mantém controles de registro e monitoramento para proteger seus ativos de informação e identificar e tratar atividades inadequadas ou não autorizadas.

## 2.8. Gestão de Vulnerabilidade e Testes de Segurança

O Programa de Gestão de Vulnerabilidades da Bitso do Brasil identifica, avalia e mitiga pontos fracos em sistemas de informação, procedimentos de segurança e controles internos, prevenindo exploração por agentes internos ou externos, incluindo ataques zero-day.

## 2.9. Backup e Recuperação de Dados

A Bitso do Brasil mantém cópias de segurança atualizadas de informações e sistemas essenciais para garantir a disponibilidade e a recuperação de dados em caso de falhas, incidentes de segurança ou desastres.

## 2.10. Programa de Continuidade de Negócios

A Companhia deve implementar e manter um Programa de Continuidade de Negócios (PCN) documentado, testado e revisado anualmente, garantindo a resiliência organizacional e a recuperação de serviços essenciais em situações de interrupção.

## 2.11. Privacidade de Dados Pessoais

A Bitso do Brasil preza pelo tratamento de dados pessoais de colaboradores, clientes e terceiros em conformidade com as políticas internas e a legislação aplicável. A Companhia assegura confidencialidade, integridade e disponibilidade dessas informações.

## 2.12. Treinamento e Divulgação

A Bitso do Brasil manterá um programa de conscientização, educação e treinamento em Segurança da Informação, com o objetivo de disseminar a cultura de segurança e avaliar o conhecimento e a maturidade dos colaboradores em relação às diretrizes e práticas de segurança. Todos os colaboradores devem participar dos treinamentos obrigatórios e de programas de educação contínua.  A Bitso do Brasil também

promoverá ações de conscientização direcionadas aos clientes, com o objetivo de incentivar o uso seguro de seus produtos e serviços.

## 3. Gestão de Segurança em Fornecedores e Prestadores de Serviços

A Bitso do Brasil, por meio de seu Processo de Gestão de Terceiros, estabelece que todos os fornecedores e prestadores de serviços que manuseiem dados sensíveis ou que sejam críticos para a continuidade operacional da Companhia devem adotar padrões de segurança da informação compatíveis e equivalentes aos controles internos da instituição.

## 4. Relatório Anual

A Companhia elaborará um Relatório Anual sobre a implementação e a efetividade do Plano de Ação e de Resposta a Incidentes, com data-base de 31 de dezembro. Este relatório será apresentado ao Conselho de Administração (ou Diretoria) até 31 de março do ano seguinte ao da data-base, para fins de supervisão e acompanhamento da Alta Administração.

## 5. Retenção Documental e Submissão à Fiscalização

Sem prejuízo de outros prazos legais ou regulatórios, os seguintes documentos devem ficar à disposição do Banco Central do Brasil pelo prazo mínimo de cinco anos:

- A Política de Segurança Cibernética e o Plano de Ação e de Resposta a Incidentes;
- Documentação detalhada dos procedimentos de *Due Diligence* e verificação prévia de fornecedores;

- Contratos de prestação de serviços relevantes e toda a documentação comprobatória de requisitos para serviços prestados no exterior.

- Os dados, os registros e as informações relativas aos **mecanismos de acompanhamento e de controle** de que trata a regulamentação aplicável, contado o prazo a partir da implementação dos citados mecanismos;
- A documentação contendo os **critérios que configurem uma situação de crise**, conforme definido nos procedimentos internos de gestão de incidentes e continuidade de negócios.

## 6. Designação do Diretor Responsável pela Segurança Cibernética

A Bitso do Brasil designará formalmente um Diretor responsável pela Política de Segurança Cibernética e pela execução do Plano de Ação e de Resposta a Incidentes. O nome do cargo e as responsabilidades específicas estão documentados em ata do órgão de administração.

## 7. Manifesto de Segurança da Informação Bitso do Brasil

Estamos desenvolvendo maneiras mais eficazes de proteger a Bitso do Brasil e ajudando outros departamentos a seguir as melhores práticas de segurança. Por meio desse trabalho, seguimos os seguintes princípios:

- **Confiança Zero:** Acreditamos que todo acesso e processo dos funcionários deve ser autenticado, autorizado e continuamente validado antes de conceder ou manter o acesso a quaisquer aplicativos e dados. Confiamos nas pessoas e nos sistemas, mas verificamos e validamos;

- **Complexidade Reduzida:** Acreditamos na inclusão de recursos de segurança desde o início do projeto, no Ciclo de Vida de Desenvolvimento de Software (SDLC). Projetaremos nossos recursos de segurança para permitir a adoção regular de novas tecnologias e a facilidade de uso. Queremos tratar a segurança como parte integrante do projeto geral do sistema;

- **Usabilidade Segura:** Acreditamos no uso de mecanismos de segurança que não tornem o recurso mais difícil de acessar do que se os mecanismos de segurança não estivessem presentes;

- **Canais de comunicação confiáveis:** Garantimos que as informações em trânsito sejam criptografadas. Partimos do princípio de que sistemas ou partes externas não são seguros;

- **Responsabilidade e rastreabilidade:** Temos a responsabilidade de proteger e controlar informações e equipamentos. Como funcionários, somos responsáveis por nossas ações e acreditamos na prevenção e detecção de usos indevidos. Quando os mecanismos de segurança não forem viáveis, tomaremos outras medidas;

- **Segurança em caso de falha e recuperação:** Acreditamos em garantir que nossos sistemas e informações sejam, e continuem sendo, resilientes diante de ameaças esperadas. Praticaremos planos de contingência e recuperação para assegurar a disponibilidade e a resiliência adequadas;

- **Procedimentos repetíveis e documentados:** Criamos documentação que contribui para a segurança e a operação do sistema. Nossa documentação nos permitirá reconstruir sistemas e processos de forma completa e correta. Pensaremos nas pessoas que usarão esses documentos e no legado que deixaremos;

- **Defesa em profundidade:** Integraremos pessoas, tecnologia e operações em múltiplas camadas para proteger a Nvio e suas informações;

- **Separação de funções:** Acreditamos que nenhum funcionário deve ter privilégios suficientes para usar o sistema indevidamente por conta própria. Mantemos o cuidado de manter a autorização e a execução separadas. Garantiremos que as pessoas e os processos certos tenham o acesso certo aos recursos certos no momento certo.

## 8. Conformidade

Todos os funcionários devem cumprir os requisitos descritos neste documento, a menos que os órgãos reguladores aos quais a Bitso do Brasil está sujeita identifiquem e exijam uma exceção. Qualquer exceção ou desvio da Política de Segurança da Informação e suas diretrizes complementares deve ser baseado em requisitos legais ou comerciais específicos.

A Bitso do Brasil reserva-se o direito de tomar medidas disciplinares contra funcionários, incluindo demissão, por qualquer desvio do conteúdo da Política de Segurança da Informação ou de qualquer outra política mencionada neste documento. Dependendo da gravidade da violação, isso poderá levar a medidas legais de acordo com a legislação local.

## 9. Monitoramento da Política

Vigência e Atualização, esta Política entra em vigor na data indicada no cabeçalho e permanecerá válida até sua revisão ou substituição. A Política de Segurança Cibernética e o respectivo Plano de Ação e Resposta a Incidentes devem ser aprovados pelo Conselho de Administração, conforme previsto na regulamentação vigente.
Sua atualização deverá ocorrer sempre que houver mudanças na legislação aplicável, alterações nos processos internos da Companhia que impactem as diretrizes aqui estabelecidas, determinações de órgãos reguladores ou, no mínimo, uma vez a cada 12 meses. Quaisquer alterações em seu conteúdo deverão ser revisadas e autorizadas pelo Departamento de Segurança da Informação em conjunto com o seu CISO.

# 10. Glossário

Esta seção tem como finalidade de esclarecer o significado dos principais termos utilizados nesta Política, garantindo entendimento uniforme sobre os conceitos relacionados à segurança da informação.

Sendo estes conceitos:

- **Ameaça**: Qualquer fator e/ou ação, isoladamente ou em conjunto, que represente uma causa potencial de um incidente indesejado capaz de interferir nos objetivos de negócio da Bitso do Brasil ou de causar danos e impactos à integridade, confidencialidade, autenticidade e disponibilidade de dados e informações. As ameaças podem ser internas ou externas, intencionais ou não intencionais;
- **Banco Central do Brasil (BACEN):** Órgão responsável por disciplinar a constituição, o funcionamento e a fiscalização das instituições financeiras e demais instituições autorizadas a funcionar, bem como pela descontinuidade da prestação de seus serviços;
- **Colaborador(es):** Pessoas físicas, administradores, bem como todos os funcionários da Companhia com vínculo empregatício, estagiários, menores aprendizes e trabalhadores efetivos ou temporários;
- **Controles de Segurança:** Medidas técnicas, administrativas, físicas e organizacionais implementadas com o objetivo de proteger os ativos de informação contra ameaças, vulnerabilidades e incidentes, assegurando a conformidade com esta Política, com as regulamentações do Banco Central do Brasil e com as demais normas aplicáveis à Bitso do Brasil;
- **Criptografia:** Prática de construir e analisar protocolos que impeçam terceiros não autorizados de acessar o conteúdo de arquivos e/ou mensagens privadas, convertendo dados de um formato legível para um formato codificado

mediante o uso de algoritmos, hashes e assinaturas digitais, com o objetivo de proteger as informações;

- **Diretoria:** Órgão composto pelos membros eleitos pelos acionistas da Companhia, por meio de ato societário devidamente registrado na junta comercial competente;
- **Incidente:** Qualquer evento que fuja à operação normal do negócio da Bitso do Brasil capaz de afetar parcial ou totalmente os serviços prestados, ocasionando interrupção, degradação ou impacto na qualidade das operações e que possa comprometer a continuidade dos serviços;
- **Incidente de Segurança Cibernética:** Evento adverso, confirmado ou sob suspeita, que comprometa ou possa comprometer a confidencialidade, integridade, disponibilidade ou autenticidade de informações, sistemas, serviços tecnológicos ou ativos digitais da Bitso do Brasil;
- **Informação:** Conjunto de dados organizados que compõem uma mensagem sobre determinado fato, processo ou evento, incluindo, quando aplicável, dados pessoais. As informações podem ser registradas, armazenadas, processadas ou transmitidas em diversos meios, físicos ou digitais como documentos impressos, sistemas eletrônicos, mídias removíveis, correio eletrônico, vídeos, comunicações orais ou outros suportes;
- **Política de Segurança da Informação (PSI):** Conjunto de diretrizes, princípios e regras formais estabelecidas pela Nvio Brasil para garantir a proteção adequada das informações sob sua responsabilidade. A PSI define responsabilidades, controles e procedimentos necessários para preservar a confidencialidade, a integridade, a autenticidade e a disponibilidade das informações, em conformidade com legislações, regulamentações e boas práticas aplicáveis;

- **Risco Cibernético:** Probabilidade de ocorrência de evento relacionado ao ambiente cibernético que possa comprometer a segurança das informações, impactar a continuidade operacional ou gerar perdas financeiras, reputacionais, regulatórias ou legais à Bitso do Brasil;
- **Terceiros:** Toda e qualquer entidade, bem como seu representante legal e/ou preposto, que preste ou esteja prestando serviços à Bitso do Brasil, incluindo prestadores de serviços, parceiros, fornecedores, auditores e demais partes relacionadas.