

	Política de Segurança da Informação	SEG-POL-001-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

Política de Segurança da Informação

Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda.

Sumário

1. Objetivo	1
2. Abrangência	1
3. Termos e Definições	2
4. Princípios de Segurança da Informação	3
5. Diretrizes Gerais	3
6. Exceções	14
7. Violações e Penalidades	14
8. Revisão	15
9. Normas de Referência	15
10. Vigência	15
11. Controle e Histórico de Versões	16

1. Objetivo

Esta Política tem como objetivo estabelecer os princípios e diretrizes de Segurança da Informação da Organização, visando proteger suas informações e ativos e assegurar sua confidencialidade, integridade e disponibilidade.

Adicionalmente, esta Política busca orientar a adoção de práticas de Segurança da Informação, promover o atendimento aos requisitos legais, regulatórios, contratuais e demais requisitos aplicáveis, bem como estabelecer as responsabilidades relacionadas à proteção das informações no âmbito da Organização.

2. Abrangência

Esta Política aplica-se a todos os colaboradores, terceiros e fornecedores que tenham acesso às informações, ativos, sistemas, serviços ou ambientes da Organização, independentemente de sua localização ou da forma de acesso.

	Política de Segurança da Informação	SEG-POL-001-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

As diretrizes estabelecidas nesta Política abrangem as informações, independentemente de seu formato físico ou digital, bem como os ativos, recursos tecnológicos, processos e ambientes utilizados para seu armazenamento, processamento ou transmissão.

A Segurança da Informação não se restringe aos sistemas e recursos tecnológicos, abrangendo também pessoas, processos e demais meios envolvidos na proteção das informações da Organização.

Este documento aplica-se à Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda. (sociedade PSAV), referida neste documento como Organização.

Para a sociedade PSAV, os requisitos de segurança cibernética da Resolução BCB nº 85/2021 são detalhados na Política de Segurança Cibernética, inclusive os de contratação de serviços de processamento, armazenamento de dados e computação em nuvem, tratados no seu Capítulo de Nuvem, à qual esta Política se articula.

3. Termos e Definições

Termo	Definição
Ativo	Qualquer elemento que tenha valor para a Organização, incluindo informações, sistemas, aplicações, serviços, infraestrutura, dispositivos, pessoas e processos.
Informação	É um conjunto de dados organizados e ordenados, de forma que seja possível a compreensão e entendimento de determinado assunto em um contexto.
Vulnerabilidade	Fragilidade ou deficiência em um ativo, processo, sistema ou controle que pode ser explorada por uma ameaça, podendo resultar em um incidente de segurança da informação.
Ameaça	Evento, ação ou agente com potencial de explorar uma vulnerabilidade e causar danos a um ativo ou à segurança da informação.
Incidente	Evento que comprometa ou possa comprometer a confidencialidade, a integridade ou a disponibilidade de informações, sistemas ou serviços da Organização.
Risco	Possibilidade de uma ameaça explorar uma vulnerabilidade e causar impacto negativo à organização, considerando a probabilidade de ocorrência e suas consequências.
Criptografia	Técnica utilizada para cifrar uma informação ou conjunto de dados, de forma que fique inacessível para os que não possuem a chave de acesso.

	Política de Segurança da Informação	SEG-POL-001-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

Termo	Definição
Backup	É a cópia de arquivos, pastas, bases de dados ou até discos inteiros para sistemas de armazenamento secundários, de forma a preservar os dados em caso de incidentes ou problemas, possibilitando sua recuperação.
Responsável pelo SGSI	Diretor responsável pelo Sistema de Gestão de Segurança da Informação e pela política de segurança cibernética perante o Banco Central do Brasil (Res. BCB 85/2021).
Responsável pela Segurança da Informação	Responsável pela gestão da segurança da informação e da segurança cibernética, inclusive pela coordenação da resposta a incidentes.
Alta Direção	Diretoria da Organização

4. Princípios de Segurança da Informação

A Segurança da Informação na Organização é orientada pela preservação da confidencialidade, integridade e disponibilidade das informações e dos ativos associados, considerando os riscos e os requisitos aplicáveis às suas atividades.

Para fins desta Política, devem ser observados os seguintes princípios:

- a. Confidencialidade:** assegurar que as informações sejam acessadas e utilizadas somente por pessoas, entidades ou processos devidamente autorizados;
- b. Integridade:** assegurar a exatidão, completude e proteção das informações contra alterações ou destruição não autorizadas;
- c. Disponibilidade:** assegurar que as informações, sistemas e recursos necessários estejam acessíveis e disponíveis às partes autorizadas, conforme as necessidades da Organização.

A aplicação desses princípios deverá considerar a criticidade das informações e dos ativos, os riscos identificados e os requisitos legais, regulatórios e contratuais aplicáveis.

5. Diretrizes Gerais

As diretrizes estabelecidas nesta Política visam orientar a proteção das informações e dos ativos da Organização contra ameaças internas e externas, reduzir os riscos decorrentes de falhas de Segurança da Informação e promover a adoção e manutenção de controles adequados às necessidades da Organização.

	Política de Segurança da Informação	SEG-POL-001-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

5.1. Objetivos de Segurança da Informação

A Organização estabelece objetivos de segurança da informação mensuráveis, coerentes com esta Política e com o apetite a risco aprovado, definidos e revisados anualmente no Plano Anual do SGSI, com indicador, meta, método de medição, responsável e prazo. O acompanhamento é reportado trimestralmente ao Comitê de Compliance e consolidado na análise crítica da direção.

5.2. Compromisso da Organização

A Organização está comprometida com a proteção de suas informações e ativos, com a manutenção e melhoria contínua da Segurança da Informação e com o atendimento aos requisitos legais, regulatórios, contratuais e demais requisitos aplicáveis.

Para tanto, a Organização deve promover a adoção de controles de Segurança da Informação proporcionais aos riscos identificados, disponibilizar os recursos necessários e fomentar uma cultura de segurança compatível com seus objetivos e atividades.

5.3. Conformidade

A Organização deve identificar e observar os requisitos legais, regulatórios, contratuais e demais requisitos aplicáveis à Segurança da Informação, adotando as medidas necessárias para assegurar sua conformidade.

A aderência aos requisitos aplicáveis deve ser acompanhada e avaliada periodicamente, devendo eventuais desvios ou não conformidades identificadas serem registrados e tratados de forma tempestiva, conforme os processos estabelecidos pela Organização.

5.4. Gestão de Riscos

A Organização deve gerenciar os riscos relacionados à Segurança da Informação de forma estruturada e proporcional ao seu contexto, considerando os impactos potenciais sobre suas informações, ativos, processos e serviços.

Os riscos identificados devem ser avaliados, tratados e monitorados conforme os critérios e diretrizes estabelecidos pela Organização, de forma a apoiar a tomada de decisão e a manutenção de níveis de risco compatíveis com seus objetivos.

5.5. Segurança em Recursos Humanos

A Organização deve adotar controles de Segurança da Informação ao longo do ciclo de vínculo dos colaboradores, desde os processos de seleção e contratação até o desligamento,

	Política de Segurança da Informação	SEG-POL-001-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

considerando as responsabilidades, os riscos e os requisitos aplicáveis às funções desempenhadas.

Os processos relacionados à gestão de pessoas devem contemplar, quando aplicável, a verificação dos candidatos, a formalização das responsabilidades e obrigações relacionadas à Segurança da Informação e a adoção de medidas adequadas nos processos de admissão, movimentação e desligamento.

As responsabilidades relacionadas à Segurança da Informação devem ser comunicadas aos colaboradores e formalizadas por meios adequados e auditáveis.

5.6. Conscientização e Treinamento

A Organização deve promover ações de conscientização e treinamento em Segurança da Informação, de forma a assegurar que os colaboradores conheçam suas responsabilidades e estejam capacitados para cumprir as diretrizes e controles aplicáveis às suas atividades.

As ações devem considerar as necessidades da Organização e, quando aplicável, as responsabilidades e os riscos associados às funções desempenhadas, contemplando treinamentos gerais e específicos.

A participação, conclusão e, quando aplicável, a efetividade das ações de conscientização e treinamento devem ser acompanhadas e registradas por meios adequados e auditáveis.

5.7. Gestão de Ativos

A Organização deve identificar, registrar e manter atualizados os ativos relevantes para suas atividades e para a Segurança da Informação, considerando informações, recursos tecnológicos, sistemas, aplicações, serviços e demais ativos que suportem seus processos e operações.

Os ativos devem possuir responsáveis definidos e ser gerenciados de acordo com sua importância, criticidade e riscos associados, considerando todo o seu ciclo de vida, desde sua aquisição, criação ou disponibilização até sua devolução, substituição ou descarte.

Os registros dos ativos devem ser periodicamente revisados e atualizados sempre que ocorrerem alterações relevantes em sua situação, utilização ou responsabilidade.

5.8. Uso Aceitável de Ativos e Recursos Tecnológicos

A Organização deve estabelecer diretrizes para o uso adequado e seguro de seus ativos e recursos tecnológicos, que devem ser utilizados prioritariamente para o desempenho das

	Política de Segurança da Informação	SEG-POL-001-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

atividades profissionais e em conformidade com os requisitos internos, legais, regulatórios e contratuais aplicáveis.

Os colaboradores e demais usuários autorizados devem utilizar os ativos, sistemas, aplicações, serviços e recursos tecnológicos de forma responsável, ética e segura, adotando os cuidados necessários para prevenir acessos não autorizados, perda, alteração, divulgação indevida ou comprometimento das informações e dos recursos da Organização.

Somente ativos, softwares, serviços e recursos tecnológicos devidamente autorizados pela Organização devem ser utilizados para armazenar, processar ou transmitir informações corporativas, observadas as exceções formalmente aprovadas.

5.9. Classificação e Rotulagem da Informação

As informações da Organização devem ser classificadas de acordo com sua sensibilidade, criticidade e requisitos de proteção, de forma a assegurar a aplicação de controles compatíveis com os riscos associados ao seu acesso, uso ou divulgação.

A classificação atribuída deve orientar o tratamento e a proteção da informação durante seu ciclo de vida e ser revisada sempre que ocorrerem alterações relevantes em sua natureza, valor, sensibilidade ou requisitos aplicáveis.

As informações devem ser rotuladas, quando aplicável, de forma a permitir a identificação de sua classificação e orientar os usuários quanto aos cuidados necessários para seu adequado tratamento.

A informação é classificada nos níveis Público, Uso Interno, Confidencial e Restrito, na forma da Norma de Gestão da Informação. Dados de operações e de clientes protegidos por sigilo (Lei Complementar nº 105/2001, estendida às sociedades PSAV pela Resolução CMN nº 5.280/2026) são classificados, no mínimo, como Confidencial, e os instrumentos de controle de ativos virtuais são classificados, em qualquer hipótese, como Restrito; o compartilhamento externo de dados sob sigilo depende de base legal, ordem de autoridade competente ou consentimento do titular.

5.10. Transferência de Informações

A transferência de informações da Organização, por meios físicos, digitais ou outros meios de comunicação, deve ser realizada de forma segura e compatível com a classificação e a sensibilidade das informações envolvidas.

	Política de Segurança da Informação	SEG-POL-001-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

Devem ser adotados controles adequados para proteger as informações durante sua transferência contra acesso não autorizado, perda, alteração, divulgação indevida ou comprometimento, considerando o meio utilizado e os riscos associados.

Quando a transferência envolver terceiros ou outras organizações, devem ser estabelecidos requisitos de proteção compatíveis com as informações compartilhadas e com a natureza do relacionamento.

5.11. Retenção e Descarte de Informações

As informações da Organização devem ser mantidas pelo período necessário ao atendimento das necessidades do negócio e dos requisitos legais, regulatórios, contratuais e demais requisitos aplicáveis.

A retenção das informações deve considerar sua natureza, classificação e finalidade, assegurando sua proteção durante todo o período em que forem mantidas pela Organização.

As informações e os meios que as armazenem devem ser descartados de forma segura quando não forem mais necessários ou quando encerrado o período de retenção aplicável, utilizando métodos compatíveis com sua classificação e sensibilidade, de forma a impedir sua recuperação ou acesso não autorizado.

Quando o descarte for realizado por terceiros, devem ser mantidas evidências de sua execução, quando aplicável.

5.12. Privacidade e Proteção de Dados Pessoais

A Organização deve assegurar a proteção dos dados pessoais tratados no âmbito de suas atividades, observando os princípios, direitos dos titulares e demais requisitos estabelecidos pela legislação e regulamentação aplicáveis à proteção de dados pessoais.

O tratamento de dados pessoais deve ser realizado para finalidades legítimas e compatíveis com as atividades da Organização, limitado ao necessário para o atendimento das finalidades estabelecidas e protegido contra acesso não autorizado, perda, alteração, divulgação ou tratamento indevido.

Devem ser adotadas medidas de segurança e proteção adequadas aos riscos associados ao tratamento de dados pessoais durante todo o seu ciclo de vida.

	Política de Segurança da Informação	SEG-POL-001-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

5.13. Propriedade Intelectual

A Organização deve proteger os direitos de propriedade intelectual relacionados às informações, sistemas, aplicações, códigos-fonte, documentações, marcas e demais ativos intelectuais utilizados, desenvolvidos ou mantidos no âmbito de suas atividades.

O uso, reprodução, alteração, distribuição ou compartilhamento de materiais protegidos por direitos de propriedade intelectual deve observar as autorizações, licenças, contratos e demais requisitos legais aplicáveis.

Os colaboradores e demais usuários autorizados devem utilizar softwares, conteúdos e outros materiais de terceiros em conformidade com os respectivos direitos de uso e licenciamento.

5.14. Gestão de Identidades e Acessos

O acesso às informações, sistemas, aplicações, serviços e recursos tecnológicos da Organização deve ser concedido de acordo com as necessidades das atividades desempenhadas, observando os princípios do menor privilégio, necessidade de conhecimento e segregação de funções.

As identidades e os acessos devem ser gerenciados durante todo o seu ciclo de vida, contemplando sua concessão, alteração, revisão e revogação, mediante autorização adequada e manutenção dos registros e evidências aplicáveis.

Devem ser adotados mecanismos de autenticação compatíveis com os riscos e a criticidade dos recursos acessados, incluindo autenticação multifator, quando aplicável.

5.15. Segregação de Funções

As funções e responsabilidades conflitantes devem ser segregadas de forma a reduzir os riscos de fraude, erro, uso indevido de informações ou execução de atividades não autorizadas.

A definição de responsabilidades, atribuições e acessos deve considerar potenciais conflitos de interesse e incompatibilidades entre atividades, observando os riscos associados aos processos e às funções desempenhadas.

Quando a segregação de funções não for viável, devem ser adotados controles compensatórios adequados aos riscos identificados.

	Política de Segurança da Informação	SEG-POL-001-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

5.16. Segurança Física e do Ambiente

A Organização deve adotar medidas de segurança física e ambiental adequadas para proteger suas informações, ativos e recursos tecnológicos contra acesso físico não autorizado, danos, interferências e demais ameaças que possam comprometer sua segurança.

O acesso às instalações e áreas que abriguem informações ou ativos relevantes deve ser controlado de acordo com os riscos e as necessidades da Organização, sendo restrito às pessoas devidamente autorizadas.

Os ativos e informações devem ser protegidos nos ambientes em que sejam utilizados ou armazenados, incluindo a adoção de práticas destinadas a prevenir exposição, acesso indevido, perda ou danos.

5.17. Teletrabalho e Acesso Remoto

O teletrabalho e o acesso remoto às informações, sistemas, aplicações e recursos tecnológicos da Organização devem ser realizados de forma segura, observando os requisitos de proteção estabelecidos e os riscos associados ao ambiente e à forma de acesso.

Os usuários devem adotar medidas adequadas para prevenir o acesso não autorizado, a exposição ou o comprometimento das informações e dos ativos da Organização durante a realização de atividades fora dos ambientes corporativos.

O acesso remoto aos recursos da Organização deve ser realizado por meios e dispositivos autorizados, utilizando os mecanismos de segurança e autenticação estabelecidos pela Organização.

5.18. Segurança de Redes e Comunicações

A Organização deve proteger suas redes, serviços de comunicação e demais recursos de conectividade contra acessos não autorizados, interceptação, indisponibilidade e outras ameaças que possam comprometer a confidencialidade, integridade ou disponibilidade das informações e dos serviços.

Os recursos de rede e comunicação devem ser gerenciados e protegidos por meio de controles compatíveis com os riscos e a criticidade dos ambientes e serviços suportados, considerando a segregação dos ambientes e a restrição das comunicações, quando aplicável.

A arquitetura, as configurações e os mecanismos de proteção das redes e comunicações devem ser periodicamente avaliados e atualizados de acordo com as necessidades da Organização e os riscos identificados.

	Política de Segurança da Informação	SEG-POL-001-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

5.19. Proteção contra Código Malicioso

A Organização deve adotar medidas para prevenir, detectar e tratar ameaças relacionadas a códigos maliciosos que possam comprometer a confidencialidade, integridade, disponibilidade das informações ou o funcionamento de seus ativos e recursos tecnológicos.

Os ativos da Organização devem ser protegidos por mecanismos de segurança compatíveis com os riscos identificados, contemplando medidas preventivas, detectivas e corretivas contra códigos maliciosos.

Os usuários devem comunicar imediatamente às áreas responsáveis qualquer suspeita ou evidência de código malicioso, comportamento anômalo ou comprometimento de ativos e recursos tecnológicos da Organização.

5.20. Gestão de Vulnerabilidades

A Organização deve identificar, avaliar, priorizar e tratar as vulnerabilidades que possam comprometer a segurança de suas informações, ativos, sistemas, aplicações e serviços, de forma compatível com os riscos identificados.

As vulnerabilidades identificadas devem ser tratadas em prazo compatível com sua criticidade e impacto potencial, adotando-se medidas de mitigação, correção ou controles compensatórios quando aplicável.

A efetividade das ações implementadas deve ser acompanhada periodicamente, de forma a apoiar a redução contínua da exposição aos riscos de Segurança da Informação.

5.21. Gestão de Mudanças

A Organização deve assegurar que as mudanças relacionadas às informações, ativos, sistemas, aplicações, infraestrutura e serviços sejam avaliadas, aprovadas, implementadas e registradas de forma controlada, considerando os riscos associados à Segurança da Informação.

As mudanças que possam impactar a confidencialidade, integridade, disponibilidade ou conformidade das informações e dos serviços da Organização devem ser submetidas à análise dos riscos e à adoção dos controles de segurança aplicáveis antes de sua implementação.

As mudanças implementadas devem ser registradas e, quando aplicável, avaliadas posteriormente, de forma a verificar sua efetividade e identificar a necessidade de ações corretivas ou de melhoria.

	Política de Segurança da Informação	SEG-POL-001-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

5.22. Monitoramento e Registro de Eventos

A Organização deve monitorar seus ativos, sistemas, aplicações, serviços e ambientes tecnológicos, de forma a identificar eventos que possam impactar a Segurança da Informação e apoiar a prevenção, detecção, investigação e tratamento de incidentes.

Os registros de eventos relevantes para a Segurança da Informação devem ser gerados, protegidos, armazenados e mantidos pelo período definido pela Organização, de forma a preservar sua integridade, disponibilidade e rastreabilidade.

As informações obtidas por meio do monitoramento e dos registros de eventos devem ser utilizadas para apoiar a gestão da Segurança da Informação, a investigação de incidentes, o atendimento a requisitos legais, regulatórios e contratuais e a melhoria contínua dos controles implementados.

5.23. Criptografia

A Organização deve adotar mecanismos criptográficos adequados para proteger a confidencialidade, integridade e autenticidade das informações, considerando sua classificação, sensibilidade, os riscos identificados e os requisitos legais, regulatórios e contratuais aplicáveis.

A utilização de controles criptográficos deve observar critérios definidos pela Organização para a proteção das informações em armazenamento, processamento e transmissão, bem como para o gerenciamento adequado das chaves criptográficas, quando aplicável.

Os mecanismos criptográficos adotados devem ser periodicamente avaliados, de forma a assegurar sua efetividade e adequação às necessidades da Organização.

5.24. Backup

A Organização deve assegurar a realização e a manutenção de cópias de segurança das informações e dos ativos necessários à continuidade de suas operações, de acordo com os requisitos do negócio e os riscos identificados.

As cópias de segurança devem ser protegidas contra acesso não autorizado, alteração, perda ou destruição e permanecer disponíveis para utilização quando necessário, observando os requisitos de retenção, armazenamento e recuperação estabelecidos pela Organização.

A efetividade dos processos de backup e recuperação deve ser periodicamente verificada, de forma a assegurar sua capacidade de atender às necessidades da Organização.

	Política de Segurança da Informação	SEG-POL-001-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

5.25. Uso de Serviços em Nuvem

A utilização de serviços em nuvem deve observar os requisitos de Segurança da Informação, privacidade, conformidade e gestão de riscos estabelecidos pela Organização, considerando a criticidade das informações e dos serviços envolvidos.

A contratação, utilização e gerenciamento de serviços em nuvem devem assegurar a adoção de controles compatíveis com os riscos identificados, bem como a proteção das informações durante todo o seu ciclo de vida.

Os serviços em nuvem utilizados pela Organização devem ser periodicamente avaliados quanto à sua segurança, conformidade e aderência aos requisitos estabelecidos pela Organização.

A contratação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem observa o Capítulo de Nuvem da Política de Segurança Cibernética.

5.26. Desenvolvimento Seguro

A Organização deve incorporar requisitos de Segurança da Informação em todas as etapas do ciclo de vida de desenvolvimento, aquisição, manutenção e alteração de sistemas, aplicações e demais soluções tecnológicas, de forma compatível com os riscos identificados.

Os sistemas e aplicações devem ser desenvolvidos, testados, implementados e mantidos de acordo com práticas de desenvolvimento seguro, observando requisitos de segurança, privacidade, qualidade e conformidade aplicáveis.

Alterações em sistemas, componentes e ambientes tecnológicos devem ser realizadas de forma controlada, preservando a integridade, a disponibilidade e a segurança das informações e dos serviços da Organização.

5.27. Gestão de Fornecedores e Cadeia de Suprimentos

A Organização deve gerenciar os riscos de Segurança da Informação relacionados aos fornecedores, parceiros e demais terceiros que tenham acesso às suas informações, ativos, sistemas ou serviços, durante todo o ciclo de vida do relacionamento.

Os fornecedores, parceiros e terceiros devem atender aos requisitos de Segurança da Informação, privacidade, conformidade e demais obrigações estabelecidas pela Organização, de acordo com a natureza dos serviços prestados, das informações tratadas e dos riscos envolvidos.

	Política de Segurança da Informação	SEG-POL-001-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

A contratação, o monitoramento e a reavaliação dos fornecedores, parceiros e terceiros devem considerar critérios de segurança compatíveis com os riscos identificados, bem como os requisitos legais, regulatórios e contratuais aplicáveis.

5.28. Continuidade de Negócios

A Organização deve estabelecer e manter processos que assegurem a continuidade de suas atividades e a recuperação de seus processos, informações, sistemas e serviços críticos diante de incidentes, interrupções ou eventos que possam comprometer seus objetivos de negócio.

Os requisitos de continuidade devem considerar os riscos identificados, os impactos sobre o negócio e a criticidade dos processos e ativos envolvidos, contemplando medidas de prevenção, resposta e recuperação compatíveis com as necessidades da Organização.

Os planos e processos relacionados à continuidade de negócios devem ser periodicamente avaliados, testados e atualizados, de forma a assegurar sua efetividade e aderência às necessidades da Organização.

5.29. Gestão de Incidentes

A Organização deve estabelecer e manter processos para identificação, registro, comunicação, avaliação, tratamento e resposta aos incidentes de Segurança da Informação, de forma a minimizar seus impactos e restabelecer as operações afetadas no menor tempo possível.

Os incidentes de Segurança da Informação devem ser comunicados tempestivamente às áreas responsáveis, registrados por meios adequados e tratados de acordo com sua natureza, criticidade e impactos potenciais.

As causas dos incidentes e as lições aprendidas devem ser analisadas, quando aplicável, visando à implementação de ações corretivas, preventivas e de melhoria contínua dos controles de Segurança da Informação.

O tratamento de incidentes observa a Norma de Gestão de Incidentes e o Plano de Ação e de Resposta a Incidentes. Os parâmetros de relevância de incidentes e a comunicação de situações de crise ao Banco Central do Brasil seguem a Política de Segurança Cibernética.

5.30. Uso de Inteligência Artificial

A utilização de soluções de Inteligência Artificial no âmbito da Organização deve observar os requisitos de Segurança da Informação, privacidade, propriedade intelectual, conformidade e gestão de riscos aplicáveis.

	Política de Segurança da Informação	SEG-POL-001-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

As informações da Organização somente poderão ser utilizadas em soluções de Inteligência Artificial de acordo com sua classificação, sensibilidade e com as autorizações estabelecidas pela Organização, sendo vedado o compartilhamento de informações cuja utilização possa comprometer a confidencialidade, integridade, disponibilidade ou os interesses da Organização.

A adoção e utilização de soluções de Inteligência Artificial deverão ser compatíveis com os riscos associados, observando os controles, restrições e diretrizes estabelecidos pela Organização.

5.31. Mudanças no SGSI

As mudanças no SGSI, escopo, estrutura documental, papéis, ferramentas de controle e processos, são planejadas, avaliadas quanto ao risco e aprovadas pelo Comitê de Compliance, com registro em ata e refletidas no Plano Anual do SGSI.

5.32. Monitoramento, Medição e Auditoria

Os indicadores de segurança da informação definidos nas políticas e normas são consolidados no Plano Anual do SGSI, apurados mensalmente pela Segurança da Informação e reportados trimestralmente ao Comitê de Compliance. O SGSI é auditado anualmente pela auditoria interna, exercida por empresa independente contratada, com apoio de Compliance quando necessário, e submetido à análise crítica da direção na forma do Regulamento Interno do Comitê de Compliance e do Manual do SGSI.

6. Exceções

As exceções a esta Política e aos normativos dela derivados são registradas, avaliadas quanto ao risco residual pela Segurança da Informação e aprovadas. Toda exceção tem prazo, controles compensatórios e responsável definidos e é registrada em sistema controlado que assegure rastreabilidade, integridade e histórico de alterações.

As exceções concedidas não eximem os responsáveis da adoção das medidas necessárias para reduzir os riscos decorrentes do seu tratamento.

7. Violações e Penalidades

O descumprimento das diretrizes estabelecidas nesta Política, bem como das normas, procedimentos e demais documentos dela derivados, poderá sujeitar os responsáveis às medidas administrativas, disciplinares, contratuais e legais cabíveis, conforme a natureza, a gravidade e os impactos da ocorrência.

	Política de Segurança da Informação	SEG-POL-001-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

Toda suspeita ou evidência de violação deverá ser comunicada às áreas responsáveis para análise, tratamento e adoção das medidas aplicáveis, observando os processos internos da Organização e a legislação vigente.

As violações poderão resultar, quando aplicável, na adoção de ações corretivas, medidas disciplinares, responsabilização civil, administrativa ou penal, bem como na rescisão de contratos ou outras medidas previstas na legislação e nos instrumentos firmados com a Organização.

8. Revisão

Este documento deve ser revisado no mínimo anualmente ou sempre que ocorrerem alterações relevantes na estrutura, nos processos, nos requisitos legais, regulatórios, contratuais ou demais requisitos aplicáveis à Organização, ou quando identificada a necessidade de sua atualização.

9. Normas de Referência

ISO/IEC 27001:2022: Segurança da informação, cibersegurança e proteção da privacidade, Sistemas de Gestão da Segurança da Informação, Requisitos.

ISO/IEC 27002:2022: Segurança da informação, cibersegurança e proteção da privacidade, Controles de Segurança da Informação.

Lei nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD).

Resolução BCB nº 520/2025: Prestação de serviços de ativos virtuais e funcionamento das sociedades prestadoras de serviços de ativos virtuais.

Resolução BCB nº 85/2021: Política de segurança cibernética e contratação de serviços de processamento, armazenamento de dados e computação em nuvem, aplicável às sociedades prestadoras de serviços de ativos virtuais pela Resolução BCB nº 552/2026, com as alterações da Resolução BCB nº 538/2025.

10. Vigência

Este documento entra em vigor na data de sua publicação, após aprovação pela Diretoria, com formalização em ata, após deliberação prévia do Comitê de Compliance, e permanece vigente até sua revisão ou revogação expressa.

	Política de Segurança da Informação	SEG-POL-001-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

11. Controle e Histórico de Versões

Versão	Data	Histórico de Alterações/Inclusões	Resp. Aprovação
1.0	15/10/2026	Emissão inicial.	Diretoria, após deliberação do Comitê de Compliance