

	Política de Segurança Física	SEG-POL-008-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

Política de Segurança Física

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 Proteção ao Ambiente Físico	3
5. Controle de Acesso Físico	3
6. Proteção do Ambiente e da Infraestrutura Física	5
7. Monitoramento	6
8. Comunicação de Incidente	6
9. Ambientes de Terceiros e Nuvem	6
10. Trabalho Remoto, Mesa Limpa e Equipamentos Fora das Instalações	7
11. Revisão	7
12. Normas de Referência	7
13. Vigência	8
14. Controle e Histórico de Versões	8

1. Objetivo

Esta Política tem como objetivo estabelecer diretrizes para o controle de acesso físico e a proteção do ambiente de trabalho da Organização, visando proteger as pessoas, os ativos e as informações, assegurar a confidencialidade, integridade e disponibilidade das informações e atender aos requisitos legais, regulatórios, contratuais e de negócio aplicáveis.

2. Abrangência

Esta Política aplica-se às instalações físicas da Organização e a todas as pessoas que as utilizem ou acessem, incluindo colaboradores, terceiros, prestadores de serviço, parceiros e visitantes, bem como aos ativos físicos e às informações sob sua responsabilidade.

	Política de Segurança Física	SEG-POL-008-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

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

3. Termos e Definições

Termo	Definição
Ativo	Qualquer recurso físico ou lógico que possua valor para a Organização e que necessite de proteção, incluindo equipamentos, documentos, informações e infraestrutura.
Ambiente Físico	Instalações, dependências e áreas utilizadas pela Organização para o desenvolvimento de suas atividades, incluindo escritórios, salas, áreas restritas e demais locais sob sua responsabilidade.
Área Restrita	Ambiente cujo acesso é controlado devido à criticidade dos ativos, informações ou serviços nele existentes, sendo permitido apenas às pessoas devidamente autorizadas.
Controle de Acesso Físico	Conjunto de medidas destinadas a controlar e registrar o acesso de pessoas às instalações ou áreas da Organização, de forma compatível com os riscos identificados.
Visitante	Pessoa que não integra o quadro de colaboradores da Organização e que acessa suas instalações de forma temporária, mediante autorização.
Terceiro	Pessoa física ou jurídica que presta serviços ou executa atividades para a Organização sem vínculo empregatício direto.
Perímetro de Segurança	Limite físico definido para proteger instalações, áreas ou ativos da Organização contra acessos não autorizados.
Infraestrutura Física	Conjunto de instalações, equipamentos e recursos físicos que suportam as operações da Organização, incluindo sistemas de energia, climatização, cabeamento, monitoramento e demais elementos relacionados ao ambiente físico.
Monitoramento	Acompanhamento contínuo ou periódico dos controles de segurança física e ambiental, com o objetivo de identificar eventos, falhas ou situações que possam comprometer a segurança da informação.

	Política de Segurança Física	SEG-POL-008-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

4. Princípios de Proteção ao Ambiente Físico

O ambiente físico da organização constitui parte integrante do Sistema de Gestão de Segurança da Informação (SGSI), devendo ser protegido de forma a preservar as pessoas, os ativos de informação, a infraestrutura e os serviços essenciais ao negócio.

A proteção do ambiente físico deve observar no mínimo os seguintes princípios:

- a.** Classificação por criticidade e risco, considerando o tipo de informação processada, armazenada e acessada no local;
- b.** Defesa em camadas, combinando controles físicos, administrativos e tecnológicos de natureza preventiva, detectiva e corretiva;
- c.** Acesso mínimo necessário, alinhado às funções e responsabilidades;
- d.** Proporcionalidade, garantindo que os controles sejam adequados ao nível de risco identificado;
- e.** Integração ao SGSI, aos processos de gestão de riscos, continuidade de negócios e resposta a incidentes.

Áreas que armazenem ativos de informação, tratem informações classificadas ou suportem serviços críticos devem possuir controles físicos compatíveis com sua criticidade e os riscos identificados.

5. Controle de Acesso Físico

O acesso físico às instalações corporativas deve ser controlado de forma a prevenir acessos não autorizados, proteger pessoas, ativos, informações e reduzir os riscos de segurança da informação. Considerando este fim, a organização deve:

- a.** Definir e manter o perímetro físico das instalações sob sua responsabilidade;
- b.** Controlar os pontos de entrada e saída das instalações, conforme sua criticidade e os riscos identificados;
- c.** Aplicar mecanismos de controle de acesso físicos adequados ao risco.

5.1. Gestão de acessos

O acesso às instalações da Organização deve ser concedido exclusivamente a pessoas autorizadas, com base no princípio do menor privilégio e na necessidade de acesso para o desempenho de suas atividades.

	Política de Segurança Física	SEG-POL-008-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

A Organização deve implementar mecanismos de controle de acesso físico compatíveis com a criticidade das áreas e os riscos identificados, incluindo, quando aplicável:

- a.** Portaria controlada, catracas ou sistemas equivalentes;
- b.** Credenciais físicas, identificação biométrica, cartões de proximidade (RFID) ou mecanismos equivalentes;
- c.** Trancas físicas ou eletrônicas para proteção de áreas restritas;
- d.** Barreiras físicas para proteção de acessos alternativos, como portas, janelas e acessos de serviço.

O acesso de terceiros, visitantes e prestadores de serviço deve ser previamente autorizado e concedido apenas quando necessário, preferencialmente por período determinado. Esses acessos devem ser registrados e, quando aplicável, supervisionados durante sua permanência nas instalações, sendo encerrados ou revogados ao término da necessidade de acesso.

Os acessos físicos concedidos são revisados semestralmente pela Liderança, com apoio da Segurança da Informação, e revogados quando deixarem de ser necessários.

5.2. Áreas Restritas

As áreas classificadas como restritas ou críticas devem possuir controles físicos compatíveis com sua criticidade e com os riscos identificados, de forma a prevenir acessos não autorizados e proteger os ativos e informações nelas existentes.

O acesso a essas áreas deve ser concedido exclusivamente às pessoas autorizadas para o desempenho de suas atividades e, quando aplicável, ser registrado e supervisionado conforme os procedimentos estabelecidos pela Organização.

5.3. Registro e Monitoramento

A organização deve manter registros dos acessos às áreas que possuam mecanismos de controle de acesso físico, de forma manual ou eletrônica, contendo, sempre que aplicável, informações suficientes para assegurar sua rastreabilidade, incluindo:

- a.** Identificação da pessoa;
- b.** Data e hora de entrada e saída;
- c.** Área ou local acessado.

Os registros de acesso devem ser protegidos contra acesso, alteração ou exclusão não autorizada, observando a retenção de 12 meses, conforme o Anexo B da Norma de Gestão

	Política de Segurança Física	SEG-POL-008-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

Documental, e possibilitando sua utilização em auditorias, investigações ou outras atividades de verificação, quando necessário.

O controle de acesso físico e os respectivos mecanismos de registro devem ser avaliados periodicamente quanto à sua eficácia e revisados sempre que houver mudanças relevantes na infraestrutura, no modelo de trabalho, nos riscos identificados ou após a ocorrência de incidentes de segurança da informação relacionados ao ambiente físico.

6. Proteção do Ambiente e da Infraestrutura Física

A organização deve implementar controles para proteger o ambiente físico e a infraestrutura contra ameaças físicas e ambientais que possam comprometer a segurança da informação, os ativos da Organização ou a continuidade das operações.

As medidas devem ser implementadas conforme a avaliação dos riscos relacionados ao ambiente físico, levando em conta a criticidade dos ativos presentes, o tipo de operação realizada no local e a possibilidade de ocorrência de eventos que possam causar interrupções, danos ou perda de informação, tais como:

- a.** Falhas elétricas;
- b.** Incêndios;
- c.** Alagamentos;
- d.** Condições estruturais e ambientais.

A Organização deve adotar controles físicos e ambientais compatíveis com os riscos identificados, podendo incluir, quando aplicável:

- a.** Controles para mitigação de falhas no fornecimento de energia elétrica;
- b.** Sistemas adequados de detecção, combate e supressão de incêndio;
- c.** Medidas de proteção contra alagamentos e outros eventos ambientais;
- d.** Proteção da infraestrutura elétrica, lógica e de comunicações;
- e. Proteção física dos ativos críticos contra danos acidentais ou intencionais;**
- f.** Retirada de equipamentos das instalações somente mediante registro no inventário de ativos;
- g.** Manutenção de equipamentos registrada e executada por fornecedor autorizado;
- h.** Trabalho em áreas seguras (sala de servidores ou rack, se houver) somente acompanhado por pessoa autorizada.

	Política de Segurança Física	SEG-POL-008-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

7. Monitoramento

A Organização deve monitorar os controles de segurança física e ambiental de forma compatível com os riscos identificados, visando detectar eventos de segurança, falhas nos controles implementados e situações que possam comprometer a proteção dos ativos e das informações.

A organização deve:

- a.** Implementar mecanismos de monitoramento compatíveis com a criticidade das áreas protegidas, incluindo, quando aplicável, sistemas de CFTV, alarmes, sensores ou controles equivalentes;
- b.** Proteger os sistemas e registros de monitoramento contra acesso, alteração ou exclusão não autorizada;
- c.** Realizar verificações ou testes periódicos da efetividade dos controles físicos e ambientais implementados;
- d.** Registrar, avaliar e tratar as falhas identificadas, conforme os processos estabelecidos pela Organização.

Os registros de monitoramento devem ser protegidos, possuir período de retenção de 12 meses para registros de acesso e 90 dias para imagens, conforme o Anexo B da Norma de Gestão Documental, e permanecer disponíveis para auditorias, investigações e demais necessidades de verificação, quando aplicável.

8. Comunicação de Incidente

Eventos relacionados a acessos não autorizados, intrusões, falhas nos controles físicos ou ambientais e demais situações que possam comprometer a segurança da informação devem ser comunicadas pelos canais formais definidos pela Organização e, quando caracterizados como incidentes de segurança da informação, tratados conforme o processo de gestão de incidentes vigente.

Quando o evento puder impactar a continuidade das operações, deverão ser observados os procedimentos estabelecidos para a gestão da continuidade de negócios, quando aplicável.

9. Ambientes de Terceiros e Nuvem

A segurança física dos centros de dados que hospedam os ambientes de produção da Organização é de responsabilidade dos provedores de serviços em nuvem contratados como serviços relevantes e é evidenciada por relatórios de auditoria independente (SOC 2) e

	Política de Segurança Física	SEG-POL-008-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

certificações (ISO/IEC 27001) obtidos e analisados na forma do Capítulo de Nuvem da Política de Segurança Cibernética (Seção 11.2).

10. Trabalho Remoto, Mesa Limpa e Equipamentos Fora das Instalações

As diretrizes de trabalho remoto, mesa limpa e tela limpa e de proteção dos equipamentos fora das instalações constam da Política de Trabalho Seguro e da Norma de Dispositivos e Uso Aceitável, que fixam os parâmetros de bloqueio automático de tela, criptografia de disco e gerenciamento de dispositivos. A perda ou o furto de equipamentos é registrado e comunicado imediatamente como incidente de segurança da informação.

11. Revisão

Este documento deve ser revisado no mínimo anualmente ou sempre que ocorrerem alterações relevantes no contexto da organização, nos requisitos legais, regulatórios ou contratuais aplicáveis.

12. 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.

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.

	Política de Segurança Física	SEG-POL-008-FIN
Data da Publicação: 15/10/2026	Segurança da Informação	Público

13. 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.

14. 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