# Política de Segurança da Informação, Comunicação e Privacidade

| | | |
|---|---|---|
| **Código IPT:** 18922 | **Revisão:** 00 | **Data de Aprovação:** 23/01/2024 |
| **Elaborado por:** Comitê de Segurança de Informação | | **Aprovado por:** Conselho de Administração do IPT |

Sumário

## 1 JUSTIFICATIVA

Para cumprir a missão, visão e valores do IPT, é importante que a segurança das informações produzidas pelo Instituto seja adequada. Isso garante a proteção de ativos de informação, preserva a propriedade intelectual, contribui para a conformidade regulatória, constrói confiança e reputação, mitiga riscos legais e previne e responde a incidentes de segurança.

## 2 OBJETIVO

Definir diretrizes estratégicas, responsabilidades e competências visando assegurar a disponibilidade, integridade, confidencialidade e autenticidade dos dados, informações, documentos e conhecimentos produzidos, armazenados ou transmitidos por qualquer meio dos sistemas de informação do IPT.

## 3 ABRANGÊNCIA

A Política de Segurança da Informação, Comunicação e Privacidade (PSICP) do IPT aplica-se a:

- Todos os administradores, fiscais, membros de Comitês, empregados, servidores de outros órgãos que estejam atuando junto ao Instituto, estagiários, aprendizes, bolsistas, prepostos, parceiros, fornecedores e terceiros a serviço do IPT conforme especificado nos instrumentos contratuais e negociais firmados com o IPT;
- Todos os ambientes físicos, computacionais e ativos da informação pertencentes ao Instituto ou que estejam sob sua responsabilidade;
- Todos os contratos, convênios, acordos, termos e demais instrumentos de natureza similar celebrados pelo Instituto;
- Todos os tipos e naturezas de informações geradas ou processadas pelo IPT, seja em formato eletrônico, impresso ou verbal. Isso inclui, mas não se limita a, informações contábeis, financeiras, administrativas, gerenciais, estratégicas, de pesquisa e quaisquer outras que possam ser consideradas sensíveis ou confidenciais para o Instituto.

## 4 PRINCÍPIOS E OBJETIVOS

A segurança da informação é caracterizada pelo dever de observância dos seguintes princípios:

- Confidencialidade: Garante que o acesso às informações seja efetuado somente pelas pessoas autorizadas, durante o período necessário;
- Integridade: Garante que a informação esteja íntegra e completa durante todo o ciclo de vida;
- Disponibilidade: Garante que a informação esteja disponível para as pessoas autorizadas, sempre que houver necessidade.

A segurança da informação, ainda, é caracterizada pelo dever de observância dos seguintes objetivos:

- A preservação da imagem do Instituto e de seus empregados, colaboradores, todos os administradores, fiscais, membros de Comitês e partes interessadas;
- A proteção dos dados pessoais para a garantia dos direitos individuais e coletivos das pessoas à inviolabilidade de sua privacidade e intimidade;
- A disseminação da cultura de segurança da informação e comunicações;
- A adequação do nível, da complexidade e dos investimentos em ações da Segurança da Informação, Comunicação e Privacidade ao valor dos ativos e informações, considerando os riscos a que estão expostos;
- A efetiva incorporação da Segurança da Informação, Comunicação e Privacidade desde a concepção e por todo o ciclo de vida da informação, em todos os processos executados no IPT.

## 5 REFERÊNCIAS

- Norma ABNT NBR ISO 27002:2022, que fornece os controles de Segurança da informação, Segurança Cibernética e Proteção à Privacidade;
- Norma ABNT NBR/ISO/IEC 27001:2013, que estabelece os elementos de um Sistema de Gestão de Segurança da Informação, Segurança Cibernética e Proteção à Privacidade;
- Norma ABNT NBR/ISO/IEC 22313:2020, que institui o código de melhores práticas para Gestão de Continuidade de Negócios;
- Norma ABNT NBR ISO/IEC 27005:2019, que fornece as diretrizes para a Gestão de Riscos de Segurança da Informação, Segurança Cibernética e Proteção à Privacidade;
- Norma ABNT NBR ISO/IEC 27701:2019, que fornece as diretrizes para a Gestão da Privacidade da Informação;
- Marco Civil da Internet – Lei 12.965/2014;
- Lei Geral de Proteção de Dados – Lei Federal nº 13.709, de 14/08/2018;
- Lei de Acesso à Informação – Lei 12.527, de 18/11/2011.
- Decreto estadual nº 48.987/2004, que dispõe sobre os Arquivos Públicos, os documentos de arquivo e sua gestão, os Planos de Classificação e a Tabela de Temporalidade de Documentos da Administração Pública do Estado de São Paulo, define normas para a avaliação, guarda e eliminação de documentos de arquivo;
- Decreto estadual nº 58.052/2012, que regulamenta a Lei federal n° 12.527, de 18 de novembro de 2011, que regula o acesso a informações, e dá providências correlatas;

- Decreto estadual nº 64.790/2020, que institui a Central de Dados do Estado de São Paulo - CDESP, a Plataforma Única de Acesso - PUA e o Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo, e dá providências correlata;
- Decreto estadual nº 65.347/2020, que dispõe sobre a aplicação da Lei federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), no âmbito do Estado de São Paulo;
- Deliberação Normativa CGGDIESP-1, de 30 de dezembro de 2021, que institui a Política de Governança de Dados e Informações - PGDI, no âmbito da Administração Pública Estadual, e dá providências correlatas;
- Deliberação Normativa CGGDIESP-2, de 30 de dezembro de 2021, que institui a Política de Proteção de Dados Pessoais - PPDP, no âmbito da Administração Pública Estadual, e dá providências correlatas;
- Decreto estadual nº 67.641/2023, que dispõe sobre o uso de meio eletrônico para a formalização de processo administrativo no âmbito da Administração Pública estadual, institui o Sistema Eletrônico de Informações do Estado de São Paulo - SEI/SP e dá providências correlatas.

## 6 DIRETRIZES GERAIS

### 6.1 CONTROLES ORGANIZACIONAIS

6.1.1 Estruturação e Implementação de Políticas de Segurança da Informação:

Desenvolver implementar e manter políticas de segurança da informação claras. Definir com precisão os papéis, responsabilidades e segregação de funções. Assegurar o envolvimento da Direção e incluir requisitos de segurança nos contratos com fornecedores e clientes.

6.1.2 Gestão de Comunicações e Relações Externas:

Gerenciar a comunicação e as relações com entidades externas. Manter um fluxo adequado de informações de segurança com autoridades, grupos de interesse e fornecedores. Assegurar a segurança da informação ao utilizar serviços em nuvem.

6.1.3 Gerenciamento e Proteção de Ativos de Informação:

Identificar, classificar, proteger e controlar o acesso à informação e aos ativos associados. Gerenciar a identificação e autenticação dos usuários, assegurar a correta atribuição de direitos de acesso e proteja registros.

6.1.4 Preparação e Resposta a Incidentes de Segurança da Informação:

Preparar-se para possíveis incidentes de segurança. Responder de maneira rápida e eficaz, aprender com os incidentes ocorridos e coletar evidências. Assegurar a continuidade dos negócios em caso de disrupções.

6.1.5 Cumprimento de Requisitos Legais e Normativos:

Estar em conformidade com todas as leis, regulamentos e contratos relacionados à segurança da informação, propriedade intelectual, proteção de dados pessoais e privacidade. Realizar revisões independentes para assegurar a conformidade e documentar os procedimentos operacionais.

## 6.2 CONTROLES DE PESSOAS

6.2.1 Seleção e Contratação Cuidadosa:

Definir critérios objetivos para a seleção, considerando a segurança da informação. Centrar os termos do contrato na segurança das informações da empresa.

6.2.2 Educação e Conscientização em Segurança da Informação:

Implementar programas regulares de treinamento em segurança da informação para todos os funcionários e manter um registro dessas atividades.

6.2.3 Implementação de Processos Disciplinares Claros:

Nas violações de segurança da informação, aplicar ações disciplinares, nos termos do Código de Conduta e Integridade. Realizar investigações completas e aplicar ações corretivas de maneira imparcial.

6.2.4 Gestão de Mudanças Contratuais e Manutenção da Confidencialidade:

Na alteração ou término do contrato de trabalho, revisar ou remover os acessos. Continuar a enfatizar a obrigação de confidencialidade após o término do contrato, incluindo acordos de não divulgação.

6.2.5 Estabelecimento de Políticas para Trabalho Remoto e Relato de Incidentes de Segurança:

Implementar políticas e diretrizes para o trabalho remoto com ênfase na segurança da informação. Estabelecer um processo seguro para relatar e registrar incidentes de segurança da informação.

## 6.3 CONTROLES FÍSICOS

6.3.1 Estabelecer medidas de segurança física

Implementar medidas de segurança física para proteger as instalações e impedir o acesso não autorizado. Estabelecer barreiras físicas, como cercas, portões e barreiras de acesso, para evitar a entrada de pessoas não autorizadas. Implementar sistemas de controle de acesso físico, como cartões de acesso, senhas ou sistemas biométricos, para assegurar que apenas indivíduos autorizados possam entrar nas áreas restritas.

6.3.2 Implementar controles de acesso físico e monitoramento adequados

Assegurar um controle de acesso físico adequado e um monitoramento eficiente. Implementar sistemas de controle de acesso físico, como fechaduras e sistemas de

autenticação, para assegurar que apenas pessoas autorizadas tenham permissão para entrar em áreas restritas. Estabelecer sistemas de monitoramento, como câmeras de segurança, alarmes e detector de presença para identificar e registrar atividades suspeitas.

6.3.3 Assegurar o armazenamento adequado e a proteção de informações

Proteger as informações, especialmente as sensíveis, para preservar a confidencialidade e integridade dos dados. Assegurar o armazenamento adequado das informações eletrônicas ou em papel. Manter os espaços de trabalho organizados e livres de documentos ou informações expostas.

6.3.4 Prevenir e mitigar ameaças físicas e ambientais

Realizar avaliações para identificar ameaças relevantes, como incêndios e inundações e implementar medidas preventivas correspondentes. Incluir a instalação de sistemas de detecção e combate a incêndios e a inundações, alarmes e outras medidas apropriadas para minimizar os riscos.

6.3.5 Estabelecer práticas adequadas de manutenção, descarte e reciclagem de equipamentos, mobiliários obsoletos e papéis.

Gerir adequadamente os equipamentos para assegurar seu funcionamento correto e a proteção de dados. Estabelecer práticas de manutenção regular para evitar falhas inesperadas dos dispositivos de segurança patrimonial que possam resultar na perda de dados ou interrupção das operações. Implementar processos seguros para o descarte ou reciclagem de equipamentos, garantindo que todas as informações sejam adequadamente removidas antes da disposição.

## 6.4 CONTROLES TECNOLÓGICOS

6.4.1 Proteção de Dispositivos *Endpoint*, Segurança de Redes e Filtragem da Web

Implementar controles de segurança efetivos e multifacetados em dispositivos *endpoint*, redes e serviços de rede, garantindo a integridade das informações. Utilizar soluções de segurança, incluindo antivírus, firewalls, sistemas de detecção/prevenção de intrusões e criptografia, além de manutenções e atualizações regulares do sistema operacional e de softwares. Utilizar a segregação e filtragem de redes, para controlar o tráfego e prevenir a disseminação lateral de ameaças, e filtragem da web para impedir o acesso a recursos web maliciosos ou não autorizados. Realizar monitoramento e auditorias frequentes para identificar atividades suspeitas ou não conformes.

6.4.2 Controle de Acesso, Autenticação e Uso de Criptografia

Regular o acesso a informações sensíveis, sistemas e códigos-fonte. Implementar direitos de acesso privilegiados para usuários autorizados, mecanismos robustos de autenticação, como a autenticação multifator, e o uso de senhas fortes com trocas regulares. Restringir

acesso à informação e ao código-fonte, e a aplicação de classificações de sensibilidade para definir os controles de acesso. Utilizar criptografia adequada para proteger a confidencialidade, autenticidade e integridade das informações. Monitorar e auditar constantes a fim de detectar qualquer atividade suspeita ou uso indevido dos privilégios de acesso.

6.4.3 Gestão de Capacidade, Proteção contra *Malware*, *Backup*, Redundância, Log, Monitoramento e Sincronização do Relógio

Assegurar uma gestão eficiente de recursos, incluindo a avaliação e planejamento de demandas de capacidade e implementação de processos de escalonamento. Direcionar a proteção contra *malware*, incluindo a atualização regular de soluções de segurança e varreduras periódicas para identificar e remover infecções. Regular realização de backups e testes de restauração são orientados para assegurar a recuperação de dados em caso de perda. Implementar redundância em recursos críticos e testes regulares de falhas para assegurar a continuidade das operações. Gerar registro de logs, além do monitoramento constante para detectar comportamentos anômalos, são exigidos para fornecer evidências em caso de investigações de segurança. Sincronizar relógios dos sistemas para correlacionar e analisar corretamente eventos de segurança.

6.4.4 Gerenciamento de Vulnerabilidades e Controles Operacionais

Implementar estratégia abrangente para identificar, priorizar e remediar vulnerabilidades técnicas, bem como gerenciar e monitorar configurações de hardware, software, serviços e redes. Controlar e monitorar o uso de programas utilitários privilegiados, implementar medidas de segurança para preservar a integridade dos sistemas operacionais e a separação de ambientes de desenvolvimento, teste e produção. Gerenciar mudanças, incluindo avaliações de impacto de segurança e aprovações antes da implementação. Assegurar a transparência e rastreabilidade necessárias para prevenir e investigar incidentes de segurança da informação.

6.4.5 Controle, Proteção e Testes de Dados

Assegurar a proteção adequada dos dados durante todo o ciclo de vida do desenvolvimento e operação de software e sistemas, incluindo exclusão e mascaramento de dados sensíveis, bem como a implementação de medidas para prevenir vazamentos de dados. Realizar integração de práticas de segurança desde a concepção até a manutenção do software, incluindo o uso de codificação segura e testes de segurança regulares. Exigir que os requisitos de segurança sejam cumpridos pelos fornecedores terceirizados. Utilizar dados fictícios ou mascarados para testes e a proteção adequada das informações de teste. Minimizar o impacto das atividades de auditoria nos sistemas operacionais e processos de negócios.

## 7. RESPONSABILIDADES

### 7.1 Conselho de Administração

O Conselho de Administração tem as seguintes responsabilidades:

- Aprovar as diretrizes gerais de Segurança da Informação do IPT;
- Supervisionar as atividades relacionadas ao gerenciamento de Segurança de Informação executadas pela Diretoria;
- Avaliar e tomar decisões para a adequação da estrutura destinada ao processo de gerenciamento de Segurança da Informação.

### 7.2 Diretoria

A Diretoria Executiva tem as seguintes responsabilidades:

- Propor a visão e estratégia do Instituto em relação à segurança da informação e privacidade, com apoio do Comitê;
- Definir políticas e diretrizes para proteção de dados e informações confidenciais.
- Alocar recursos adequados para implementar medidas de segurança e privacidade.
- Assegurar que a cultura de segurança seja promovida em todo o Instituto.
- Monitorar o desempenho das medidas de segurança e privacidade e realizar ajustes quando necessário.

### 7.3 Comitê de Segurança da Informação

O Comitê de Segurança da Informação, indicado pela Diretoria, tem as seguintes responsabilidades:

- Propor à Diretoria a Política de Segurança da informação e suas alterações;
- Propor à Diretoria normativos e procedimentos complementares à Política;
- Orientar a melhoria de processos e sistemas, bem como propor o desenvolvimento de políticas específicas relacionadas à segurança da informação;
- Propor iniciativas para fomentar a adoção de práticas que busquem a proteção do patrimônio institucional, a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações produzidas e o aperfeiçoamento da segurança da informação do Instituto.
- Propor ações de comunicação, conscientização e treinamentos;
- Fomentar treinamentos de conscientização em segurança para todos os usuários.

## 8. CASOS NÃO PREVISTOS NESTA POLÍTICA

Casos não previstos nesta Política serão analisados pelo Comitê de Segurança da Informação e submetidos para apreciação da Diretoria a quem caberá a indicação das providências, se necessárias.

## 9. ATUALIZAÇÃO

A PSICP será atualizada no mínimo a cada 12 meses e alterada, mediante deliberação do Conselho de Administração, sempre que necessário.