

	SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE	POL-01.1
	Política de Segurança da Informação TELTEX	Página: 1 de 5
Nível de Acesso: Público		

Aprovação	Rev:	Data	Natureza das Alterações
Alta Direção / DPO / TI	00	02/09/2025	Versão inicial para publicação pública
Alta Direção / DPO / TI	00	14/08/2026	Revisado política SGSIP

1. Apresentação

A **TELTEX TECNOLOGIA S.A.**, por meio desta Política, estabelece as diretrizes e critérios para a **Segurança da Informação e Privacidade**, reafirmando seu compromisso com a proteção das informações, dos dados pessoais, dos dados pessoais sensíveis, das imagens captadas e dos registros operacionais sob sua responsabilidade.

Esta Política integra os requisitos da ISO/IEC 27001, da ISO/IEC 27701, da Lei Geral de Proteção de Dados Pessoais — LGPD, bem como demais requisitos legais, estatutários, regulamentares, contratuais e normativos aplicáveis às atividades da **TELTEX**.

Para fins desta Política, o sistema de gestão integrado passa a ser denominado **Sistema de Gestão de Segurança da Informação e Privacidade — SGSIP**, contemplando, de forma integrada, os controles de segurança da informação e os controles de privacidade aplicáveis às operações da organização.

A **TELTEX** compromete-se com a **melhoria contínua do SGSIP**, visando assegurar a confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade e privacidade das informações tratadas em seus processos, sistemas, ambientes físicos, tecnológicos e operacionais.

O SGSIP tem como principais objetivos:

Proteger dados pessoais, dados sensíveis, imagens captadas e registros operacionais

- Garantir a confidencialidade das gravações, imagens, dados pessoais, dados pessoais sensíveis, informações corporativas e registros operacionais tratados pela TELTEX, prevenindo vazamentos, acessos indevidos, uso não autorizado, perda, alteração ou manipulação indevida de evidências.

Assegurar conformidade legal, regulatória, contratual e normativa

- Atender aos requisitos da LGPD, da ISO/IEC 27001, da ISO/IEC 27701 e demais obrigações aplicáveis, assegurando que as operações de tratamento de dados pessoais possuam finalidade definida, base legal adequada, controles proporcionais, retenção apropriada e evidências documentadas.

Definir responsabilidades e controles internos

- Estabelecer responsabilidades claras sobre o acesso, uso, tratamento, armazenamento, compartilhamento, retenção e descarte de informações, definindo quem pode acessar, o que pode acessar, quando, como e com qual finalidade, mantendo trilhas de auditoria e rastreabilidade das ações realizadas.

	SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE	POL-01.1
	Política de Segurança da Informação TELTEX	Página: 2 de 5
Nível de Acesso: Público		

Minimizar riscos operacionais, tecnológicos e de privacidade

- Identificar, avaliar e tratar riscos relacionados à segurança da informação, privacidade, continuidade dos serviços, acessos indevidos, falhas técnicas, ataques cibernéticos, sabotagens, incidentes, indisponibilidades e uso inadequado de informações, sistemas e recursos tecnológicos.

Promover cultura de segurança da informação e privacidade

- Conscientizar colaboradores, prestadores de serviço e partes interessadas quanto às boas práticas, ética, confidencialidade, responsabilidade no uso das informações, proteção de dados pessoais, mesa limpa, tela limpa, comunicação segura e reporte de incidentes ou suspeitas.

Garantir disponibilidade, integridade e continuidade dos sistemas

- Manter os sistemas, serviços e recursos tecnológicos da **TELTEX** funcionando de forma contínua, segura e confiável, prevenindo perdas de dados, indisponibilidades, falhas operacionais, apagões, erros humanos ou eventos que possam comprometer a continuidade das operações.

Responder a incidentes com agilidade, precisão e responsabilidade

- Estabelecer diretrizes para identificação, comunicação, registro, análise, contenção, tratamento e aprendizado com incidentes de segurança da informação e privacidade, protegendo os direitos dos titulares de dados, os interesses dos clientes, a continuidade dos serviços e a reputação da **TELTEX**.

Estas diretrizes devem ser lidas, compreendidas e seguidas pelos colaboradores, prestadores de serviço, provedores de produtos e serviços externos pertinentes, para que os principais ativos da **TELTEX**, incluindo informação, software e hardware, tenham o grau de confidencialidade, integridade, disponibilidade e autenticidade exigidos.

2. Escopo para aplicação

Esta política aplica-se, de forma proporcional às responsabilidades e ao relacionamento com a **TELTEX**, a:

- colaboradores, prestadores de serviços internos e terceiros autorizados;
- provedores externos, parceiros comerciais e fornecedores com acesso a informações ou ambientes da **TELTEX**;
- clientes e usuários de serviços, quando aplicável ao relacionamento contratual;
- visitantes, usuários ocasionais e demais partes interessadas que possam acessar informações, instalações, sistemas ou recursos da organização.

Os controles técnicos, procedimentos operacionais, formulários, registros e matrizes de responsabilidade aplicáveis são mantidos em documentação interna controlada.

	SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE	POL-01.1
	Política de Segurança da Informação TELTEX	Página: 3 de 5
Nível de Acesso: Público		

3. Compromisso da Teltex

A **TELTEX** compromete-se a:

- proteger informações próprias, de clientes, colaboradores, parceiros e terceiros;
- preservar a confidencialidade, integridade e disponibilidade das informações e dos ativos associados;
- tratar dados pessoais conforme finalidades legítimas, bases legais aplicáveis e requisitos da LGPD;
- adotar práticas de segurança compatíveis com a criticidade das informações e dos serviços;
- promover conscientização e responsabilidade no uso de informações e recursos tecnológicos;
- gerenciar riscos, incidentes, fornecedores e continuidade de serviços de forma planejada e controlada;
- manter processos de análise crítica, auditoria, monitoramento e melhoria contínua do sistema de gestão.

4. Princípios da Segurança da Informação

Princípio	Diretriz pública
Confidencialidade	As informações devem ser acessadas somente por pessoas autorizadas e conforme necessidade relacionada à atividade executada.
Integridade	As informações devem ser mantidas corretas, completas, protegidas contra alteração indevida e rastreáveis quando aplicável.
Disponibilidade	As informações, sistemas e recursos necessários à operação devem estar disponíveis aos usuários autorizados nos momentos requeridos.
Privacidade e proteção de dados pessoais	Os dados pessoais devem ser tratados com finalidade definida, base legal aplicável, necessidade, segurança, transparência e retenção adequada.
Responsabilização e rastreabilidade	A TELTEX busca manter evidências, registros e controles proporcionais aos riscos, preservando a rastreabilidade das ações relevantes.

5. Diretrizes gerais de uso e proteção da informação

- As informações devem ser utilizadas apenas para finalidades legítimas, autorizadas e relacionadas às atividades da **TELTEX**.
- O acesso a sistemas, documentos, ambientes físicos ou digitais devem observar autorização, necessidade de uso e responsabilidades definidas.
- Não é permitido compartilhar informações, documentos, credenciais, imagens, registros operacionais ou dados pessoais de forma indevida, pública ou sem autorização.

	SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE	POL-01.1
	Política de Segurança da Informação TELTEX	Página: 4 de 5
Nível de Acesso: Público		

- Informações classificadas como internas, restritas, confidenciais ou que contenham dados pessoais devem ser protegidas contra exposição, perda, alteração ou acesso indevido.
- O uso de recursos tecnológicos, serviços em nuvem, dispositivos e canais de comunicação deve seguir diretrizes corporativas e controles estabelecidos pela **TELTEX**.
- Situações suspeitas, fragilidades, incidentes ou potenciais violações devem ser comunicadas pelos canais internos definidos pela organização.

6. Diretrizes e proteção de dados pessoais

A **TELTEX** trata dados pessoais de acordo com a legislação aplicável, incluindo a **Lei Geral de Proteção de Dados Pessoais (LGPD)**, bem como diretrizes internas de segurança da informação e privacidade.

As atividades de tratamento devem observar, quando aplicável:

- finalidade específica e legítima;
- base legal pertinente;
- coleta limitada ao necessário;
- controle de acesso e compartilhamento;
- retenção compatível com a finalidade, obrigações legais, regulatórias ou contratuais;
- descarte, anonimização ou eliminação segura quando aplicável;
- atendimento aos direitos dos titulares, conforme canais e fluxos definidos pela organização.

Canal de privacidade e comunicação com o Encarregado/DPO:
mariana.duardes@teltex.com.br

7. Diretrizes para fornecedores, parceiros e terceiros

Fornecedores, parceiros e terceiros que tenham acesso a informações, dados pessoais, ambientes, sistemas ou ativos da **TELTEX** devem cumprir obrigações contratuais e requisitos aplicáveis de segurança da informação, confidencialidade e proteção de dados.

A **TELTEX** pode, conforme criticidade e natureza do relacionamento, avaliar requisitos de segurança e privacidade, solicitar evidências, estabelecer cláusulas contratuais, monitorar riscos e exigir comunicação de incidentes ou alterações relevantes.

8. Segurança em serviços digitais e compartilhamento de informações

O compartilhamento de informações deve ocorrer por meios autorizados, com controle de acesso, rastreabilidade e proteção adequada ao nível de sensibilidade da informação.

- links públicos ou compartilhamentos sem controle não devem ser utilizados para informações corporativas, confidenciais ou que contenham dados pessoais;
- documentos e registros devem ser compartilhados preferencialmente com destinatários identificados e autorizados;
- serviços digitais e em nuvem devem ser utilizados conforme diretrizes corporativas, requisitos contratuais e controles internos aplicáveis;

	SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE	POL-01.1
	Política de Segurança da Informação TELTEX	Página: 5 de 5
Nível de Acesso: Público		

- o encerramento ou substituição de serviços digitais deve considerar recuperação, retenção, portabilidade, exclusão e proteção das informações.

9. Gestão de incidentes de segurança da informação

A **TELTEX** mantém diretrizes internas para identificação, comunicação, avaliação, tratamento e aprendizado de incidentes de segurança da informação e privacidade.

Qualquer suspeita de vazamento, perda, acesso indevido, indisponibilidade relevante, uso não autorizado de sistemas, exposição de dados pessoais ou violação de confidencialidade deve ser comunicada imediatamente pelos canais internos definidos pela organização. Incidentes podem ser avaliados quanto ao impacto operacional, legal, contratual, reputacional e aos direitos dos titulares de dados pessoais, com ações proporcionais ao risco identificado.

10. Continuidade, disponibilidade e resiliência

A **TELTEX** adota diretrizes para continuidade e resiliência dos serviços, considerando monitoramento de ativos e serviços críticos, cópias de segurança, disponibilidade dos ambientes tecnológicos e planos de resposta a indisponibilidades ou falhas relevantes.

Os objetivos, indicadores e metas de desempenho do sistema de gestão são acompanhados internamente, de acordo com os critérios definidos pela organização.

11. Conscientização e responsabilidades

A segurança da informação depende do comportamento de todos. Colaboradores, terceiros e demais partes aplicáveis devem conhecer e cumprir as diretrizes relacionadas à proteção das informações, confidencialidade, privacidade, uso adequado de recursos tecnológicos e comunicação de incidentes.

A **TELTEX** promove ações de conscientização e mantém diretrizes internas para capacitação, responsabilidades e compromisso com a segurança da informação e privacidade.

12. Revisão, disponibilidade e melhoria contínua

Esta política é revisada periodicamente ou sempre que houver mudanças relevantes no contexto organizacional, nos requisitos legais, regulatórios, contratuais, tecnológicos ou nos riscos relacionados à segurança da informação e privacidade.

A versão externa da política pode ser disponibilizada às partes interessadas. As versões internas completas, procedimentos, evidências, controles técnicos e registros de implementação são mantidos em ambiente controlado.