Elaboração:	Análise Crítica/Aprovação:	Rev:	Data	Natureza das Alterações
Thales Rollo	Mariana Duardes	00	02/09/2025	Versão inicial
Eduardo Damasceno	Mariana Duardes	01	14/11/2025	Inclusão dos contatos de autoridades; Segurança da informação para uso de serviços em nuvem

1. Apresentação

A **TELTEX TECNOLOGIA S.A,** vem por meio desta política estabelecer as diretrizes e critérios referentes à sua Política de Segurança da Informação reafirmando seu compromisso com os requisitos com a segurança da informação, incluindo requisitos estatutários e regulamentares, e seu compromisso com a melhoria contínua do sistema de gestão de segurança da informação (**SGSI**), visando:

Proteger dados sensíveis e imagens captadas
- Garantir a **confidencialidade** de gravações, dados pessoais e registros operacionais
- Evitar vazamentos, acessos indevidos ou manipulação de evidências

Assegurar conformidade legal e regulatória
- Atender à **LGPD** (Lei Geral de Proteção de Dados) e normas como **ISO/IEC 27001 e 27701**
- Estabelecer bases legais para o tratamento de dados (ex.: consentimento, legítimo interesse)

Definir responsabilidades e controles internos
- Estabelecer quem pode acessar o quê, quando e como
- Criar trilhas de auditoria e rastreabilidade de ações

Minimizar riscos operacionais e tecnológicos
- Prevenir ataques cibernéticos, sabotagens ou falhas técnicas
- Implementar medidas de segurança física, como por exemplo controle de acesso às salas de monitoramento)

Promover cultura de segurança entre colaboradores
- Conscientizar sobre boas práticas, ética e responsabilidade no manuseio de informações
- Reduzir riscos humanos por meio de treinamentos e protocolos claros

Garantir disponibilidade e integridade dos sistemas
- Manter os sistemas de vigilância funcionando de forma contínua e confiável
- Evitar perdas de dados por falhas, apagões ou erros operacionais

Responder a incidentes com agilidade e precisão
- Ter planos de contingência e resposta a incidentes bem definidos
- Proteger a reputação da empresa e os direitos dos clientes em caso de falhas

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

O escopo da presente Política se aplica aos seguintes players:

- **Colaboradores e prestadores de serviços internos**;
- **Provedores Externos de Produtos e Serviços com impacto na Segurança da Informação da TELTEX;**
- **Clientes da TELTEX;**
- **Visitantes e usuários ocasionais de sistemas.**

Para a correta aplicação da presente Política é necessário considerar os seguintes termos e definições:

- **sistema de gestão da segurança da informação SGSI**
  sistema de gestão da segurança da informação que considera conjunto de aplicações, serviços, ativos de tecnologia da informação ou outros componentes de manuseio de informações
- **ITAM (IT Asset Management) ou em português, Gestão de Ativos de Tecnologia da Informação**
  conjunto de práticas e processos usados para controlar, monitorar e otimizar todos os ativos de TI de uma organização, desde computadores e servidores até softwares, licenças e serviços em nuvem.
  - **MDM (Mobile Device Management) ou em português, Gerenciamento de Dispositivos Móveis**
    solução tecnológica usada por empresas para monitorar, controlar e proteger smartphones, tablets e notebooks corporativos, especialmente em ambientes com equipes remotas ou em campo.
- **dados pessoais DP**
  qualquer informação que (a) possa ser usada para identificar a pessoa natural à qual tal informação se relaciona ou (b) é ou pode ser direta ou indiretamente vinculada a uma pessoa natural
- **dado pessoal sensível**
  dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural
- **titular de DP**
  pessoa natural a quem se referem os dados pessoais (DP)
- **operador de DP**
  parte interessada na privacidade, que faz o tratamento dos dados pessoais (DP) em benefício e de acordo com as instruções de um controlador de DP
- **controlador de DP**
  pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais
- **tratamento de DP**
  toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração

- **DPO (Data Protection Officer), também chamado na LGPD de Encarregado pelo Tratamento de Dados Pessoais**
  figura central na governança da privacidade dentro das organizações, sendo responsável por ser o canal de comunicação entre a empresa, os titulares dos dados e a ANPD, orientar e aconselhar sobre práticas de proteção de dados e conformidade com a LGPD e ISO 27001 e ISO 27701, monitorar o cumprimento das políticas internas de privacidade e segurança da informação, apoiar na resposta a incidentes, dar suporte na avaliação de riscos e propor medidas para mitigar impactos à segurança da informação e privacidade
- **incidente de segurança da informação**
  um ou múltiplos eventos de segurança da informação relacionados e identificados que podem prejudicar os ativos da organização ou comprometer suas operações
- **CSIRT — Computer Security Incident Response Team, ou Equipe de Resposta a Incidentes**
  equipe especializada em responder a incidentes de segurança da informação, atuando como uma linha de defesa estratégica dentro do SGSI, sendo responsável por identificar, analisar, conter e resolver eventos que possam comprometer a integridade, confidencialidade ou disponibilidade dos ativos digitais da organização.

3. Público alvo

A presente Política se aplica a todos os colaboradores, prestadores de serviços e provedores externos, independentemente de serem residentes ou não no Brasil, incluindo suas coligadas e controladas, que estejam envolvidos em processos de negócios com a **TELTEX**, tais como: pré-qualificações e procedimentos de contratação direta, bem como aqueles que celebrem com a **TELTEX** instrumentos jurídicos em virtude de tais processos, independentemente de se tratar de processo de aquisição de bens tangíveis, intangíveis, contrato, convênio, termo de cooperação ou outro instrumento.

4. Procedimento

4.1 Princípios da Segurança da Informação

4.1.1 Confidencialidade

A **TELTEX** assegura que somente pessoas autorizadas tenham acesso à informação sob seu controle, tais como, mas não se limitando à:

Tipo de Informação	Exemplos comuns em empresas de vigilância	Titular
Dados de identificação	Nome, CPF, RG, endereço, telefone	Colaboradores, Prestadores de Serviços, Usuários dos Clientes
Dados de acesso e localização	Horário de entrada/saída, áreas visitadas	
Dados visuais	Imagens de câmeras, vídeos, capturas	

Tipo de Informação	Exemplos comuns em empresas de vigilância	Titular
Dados de comportamento	Padrões de movimentação, alertas gerados	
Dados biométricos (se aplicável)	Impressão digital, reconhecimento facial	Colaboradores, Prestadores de Serviços Internos

A **TELTEX** protege tais informações contra vazamentos, espionagem corporativa e acessos indevidos, adotando conforme sua **FORM-SGSI-06.1.03 Declaração de Aplicabilidade**:

- Controles Organizacionais;
- Controles de Pessoas;
- Controles Físicos; e
- Controles Tecnológicos.

Além disso, termos e condições de contratação são celebrados na forma de instrumentos legais para:

- **Colaboradores e Prestadores de Serviços Internos:** Termo de Confidencialidade, Não Divulgação e Segurança Da Informação
- **Provedores de Produtos e Serviços/Prestadores de Serviços Externos:** Termo de Aceite e Compromisso do Provedor Externo com as Políticas de SGSI
- **Desenvolvedores/Programadores:** Termo de Confidencialidade de Acesso ao Código-Fonte

4.1.2 Integridade

A **TELTEX** assegura que a informação permaneça precisa, completa e confiável por meio da documentação dos procedimentos de operação de seu sistema de gestão da qualidade (SGQ), com certificação de 3ª parte ISO 9001.

Alterações não autorizadas, corrupção de dados ou manipulação maliciosa são prevenidas por meio de Controles Tecnológicos que são melhor detalhados em:

- ✓ **SP.TI.DOC.005 Gestão de Ativos por meio do Software InvGate**
- ✓ **SP.TI.DOC.006 Gestão de Ativos por meio de MDM**

Além disso a **TELTEX** mantém sua **POL-05 Política de Proteção à Privacidade de Dados Pessoais** disponível à: Colaboradores e prestadores de serviços internos, Prestadores de serviços de TI, Consultorias e auditores externos, Fornecedores de software, Serviços terceirizados com acesso físico ou lógico, Serviços de comunicação e transporte de dados e Serviços jurídicos e contábeis.

4.1.3 Disponibilidade

A **TELTEX** assegura que seus ativos incluindo informação, software e hardware estejam disponíveis ao pessoal autorizado quando necessário para a operacionalização de seus serviços, podendo envolver redundância de recursos, cópias de segurança ("backups"), e planos de continuidade e recuperação de incidentes; Ver também:

- ✓ **SP.TI.DOC.002 Gestão de Incidentes de Segurança da Informação**

- ✓ **SP.TI.DOC.007 Cópia de Segurança - Backup**

4.1.4 Privacidade e proteção de dados pessoais

A **TELTEX** reconhece que quase todas as organizações tratam de dados pessoais (DP) e que que a proteção da privacidade no contexto do tratamento de DP é uma necessidade da sociedade, bem como um tópico de legislação e/ou regulamentação dedicada em todo o mundo, por isso estruturou seu Sistema de Gestão de Segurança da Informação (SGSI), de forma a permitir a adição de requisitos específicos sem a necessidade de desenvolver um novo Sistema de Gestão, mas considerando:

- uma estrutura de privacidade e os princípios estabelecidos em seu SGSI;
- conformidade com a Lei Brasileira de Proteção aos Dados Pessoais: Lei Geral de Proteção de Dados Pessoais (LGPD) Lei nº 13.709, de 14/08/2018.

Ver maiores detalhes em **POL-05 Política de Proteção à Privacidade de Dados Pessoais.**

4.2 Papéis e Responsabilidades

4.2.1 Setor de Tecnologia da Informação da TELTEX

O setor de **Tecnologia da Informação** da **TELTEX** é responsável por:

a. Definir e revisar políticas de segurança junto ao **DPO**, estabelecer diretrizes claras para o uso, armazenamento e compartilhamento de imagens de câmeras, dados de clientes e registros operacionais.
b. Avaliar riscos e vulnerabilidades por meio do FORM-SGSI-06.1.02 Análise, Avaliação e Tratamento de Riscos de SGSI, identificando pontos fracos em sistemas de monitoramento, redes internas, servidores de gravação e dispositivos móveis usados na operação.
c. Acompanhar conformidade com normas e leis, como LGPD, ISO/IEC 27001, ISO/IEC 27701 executando as disposições estabelecidas pelo DPO e Assessoria Jurídica, ajudando a assegurar que a **TELTEX** esteja em conformidade com estas e outras regulamentações aplicáveis.
d. Gerenciar incidentes de segurança conforme estabelecido no **SP.TI.DOC.002 Gestão de Incidentes de Segurança da Informação**, coordenando a resposta a vazamentos de informações, dados pessoais, imagens e outros, bem como invasões de sistemas ou uso indevido de dados de clientes.
e. Auxiliar na promoção de conscientização e treinamento, sobretudo nos aspectos técnicos, treinando e orientando técnicos, operadores de monitoramento e colaboradores e prestadores de serviço internos sobre boas práticas de segurança e privacidade.
f. Avaliar impactos de segurança da informação em projetos e mudanças tecnológicas em ambiente interno e de transmissão de dados, verificando se novas tecnologias (como reconhecimento facial ou armazenamento em nuvem) estão alinhadas com os princípios de segurança e privacidade.
g. Realizar validações internas de Políticas e Controles em SGSI, sobretudo nos controles tecnológicos apontados na **FORM-SGSI-06.1.03 Declaração de Aplicabilidade**, bem com revisão de acessos e permissões.

h. Monitorar indicadores e auditorias, acompanhar métricas de segurança da informação conforme objetivos definidos no SGSI, bem como acompanhar Auditorias de Sistemas, Auditoria Interna de SGSI, Simulações para Identificação de Vulnerabilidades (Testes de Penetração/Pentest).
i. Atuar como elo de ligação entre áreas, no que tange os assuntos relacionados à Segurança da Informação, integrando áreas como TI, jurídico, operações e RH para assegurar que a segurança da informação seja transversal.

4.2.2 Encarregado de Proteção de Dados (DPO) da TELTEX

O **DPO (Data Protection Officer)**, também chamado na **LGPD** de **Encarregado pelo Tratamento de Dados Pessoais** é a figura central na governança da privacidade dentro das organizações.

Uma vez que a **TELTEX** trata dados de imagem, considerados dados sensíveis sob certo ponto de vista, ela designou para esta função:

Mariana Duardes - ti@teltex.com.br
Rua França Pinto, 1089
Vila Mariana - São Paulo - SP
CEP: 04016-030
Tel: +55 (11) 3840.6400

O **DPO (Data Protection Officer)** ou **Encarregado pelo Tratamento de Dados Pessoais** é responsável por:

a. Ser o canal de comunicação entre a empresa, os titulares dos dados e a ANPD (ver **POL-05 Política de Proteção à Privacidade de Dados Pessoais**);
b. Orientar e aconselhar sobre práticas de proteção de dados e conformidade com a LGPD e ISO 27001 e ISO 27701 (ver **MSGSI-01 Manual do Sistema de Gestão de Segurança da Informação**);
c. Monitorar o cumprimento das políticas internas de privacidade e segurança da informação;
d. Apoiar na resposta a incidentes (ver **SP.TI.DOC.002 Gestão de Incidentes de Segurança da Informação**);
e. Dar suporte na avaliação de riscos e propor medidas para mitigar impactos à segurança da informação e privacidade (ver **SP.TI.DOC.001 Gestão de riscos e oportunidades em SGSI**)

NOTA O trabalho do DPO inclui outras funções também designadas, conforme cada caso, para estabelecer e manter contato com as autoridades relevantes:

Autoridade	Finalidade Principal	Telefone	E-mail / Site de Contato
Polícia Federal – Divisão de Crimes Cibernéticos	Investigação de crimes digitais e incidentes graves	**194 (central)**	**www.pf.gov.br**
CERT.br – Centro de Estudos,	Resposta a incidentes de	**+55 11 5509-3537**	**cert@cert.br**

Autoridade	Finalidade Principal	Telefone	E-mail / Site de Contato
Resposta e Tratamento de Incidentes	segurança da informação		
ANPD – Autoridade Nacional de Proteção de Dados	Fiscalização e orientação sobre LGPD	**+55 61 2025-9700**	**www.anpd.gov.br**
Banco Central do Brasil – Departamento de Supervisão	Comunicação de incidentes em instituições financeiras	**+55 61 3414-2153**	**www.bcb.gov.br**
Ministério Público	Atuação em defesa da sociedade e investigação de ilícitos	**+55 11 4568-7610**	**www.cnmp.mp.br**
Sabesp	Abastecimento de água e esgoto	**0800 055 0195 / WhatsApp: (11) 3388-8000**	**www.sabesp.com.br**
Telliun Algar Telecom	Serviços de telecomunicações	**SAC: 10312 / Empresas: 0800 941 2822**	**algartelecom.com.br**
TIM Brasil	Serviços de telefonia e internet	**SAC: *144 / 1056 / WhatsApp: (41) 4141-4141**	**tim.com.br**
Corpo de Bombeiros de SP	Emergências, incêndios e resgates	**Emergência: 193 / Informações: (11) 3315-9333**	**corpodebombeiros.sp.gov.br**
Defesa Civil de SP	Prevenção e resposta a desastres	**Emergência: 199 / Central: (11) 2193-8888**	**defesacivil.sp.gov.br**

4.2.3 Provedores Externos de Produtos e Serviços com impacto na Segurança da Informação da TELTEX

Os provedores externos de produtos e serviços com impacto na Segurança da Informação da **TELTEX,** independentemente de serem residentes ou não no Brasil, incluindo suas coligadas e controladas, que estejam envolvidos em processos de negócios com a **TELTEX**, tais como: pré-qualificações e procedimentos de contratação direta, bem como aqueles que celebrem com a **TELTEX** instrumentos jurídicos em virtude de tais processos, independentemente de se tratar de processo de aquisição de bens tangíveis, intangíveis, contrato, convênio, termo de cooperação ou outro instrumento, devem obedecer às cláusulas específicas em contrato bem como ao disposto na presente Política, bem como em:

- ✓ **POL-04 Diretrizes de Segurança da Informação para Provedores Externos;**
- ✓ **POL-05 Política de Proteção à Privacidade de Dados Pessoais; e**
- ✓ **SP.TI.DOC.002 Gestão de Incidentes de Segurança da Informação**

Estes documentos se encontram disponíveis no endereço eletrônico da **TELTEX** em: https://teltex.com.br

Nesta categoria se destacam:

- **Prestadores de serviços de TI:** como empresas de hospedagem, suporte técnico, cloud computing, backup e recuperação de dados.
- **Consultorias e auditores externos:** que realizam avaliações, auditorias ou suporte à implementação do SGSI.
- **Fornecedores de software:** especialmente os que fornecem sistemas integrados, ERPs, CRMs ou ferramentas que lidam com dados corporativos.
- **Serviços terceirizados com acesso físico ou lógico:** como segurança patrimonial, limpeza de ambientes com servidores, ou manutenção de equipamentos. No caso de acesso físico, considerar:
  - Recepção (1° andar)
  - Showroom (1° andar)
  - Sala Técnica (1° andar)
  - Sala Administrativa (2º andar)
  - Sala Comercial e CPD (3º andar)
- **Serviços de comunicação e transporte de dados:** como operadoras de telecomunicações ou correios que lidam com documentos confidenciais.
- **Serviços jurídicos e contábeis:** que acessam informações estratégicas, contratuais ou financeiras da empresa.

4.2.4 Colaboradores diretos e Prestadores de Serviços Internos da TELTEX

Os **Colaboradores diretos e Prestadores de Serviços Internos** da **TELTEX** são responsáveis por:

- **Cumprir integralmente a presente Política de Segurança da Informação,** seguindo todas as diretrizes, normas e procedimentos estabelecidos pela empresa;
- **Preservar a confidencialidade, integridade e disponibilidade das informações**, incluindo
  informações, imagens de câmeras, dados de clientes, registros de ocorrências, entre outros;
- **Utilizar os recursos tecnológicos de forma segura e responsável**, evitando o uso indevido de sistemas, redes e dispositivos de forma que possam comprometer a segurança da informação e privacidade de dados pessoais (ver **POL-03 Política de Uso e Conservação de Equipamentos Teltex**);
- **Reportar incidentes ou vulnerabilidades imediatamente**, incluindo quaisquer falhas, suspeitas de violação ou comportamento anômalo, comunicando ao gestor ou à **Área de Tecnologia da Informação** da **TELTEX** (ver **SP.TI.DOC.002 Gestão de Incidentes de Segurança da Informação**);
- **Participar de treinamentos e ações de conscientização** promovidos e/ou indicados pela **TELTEX**, mantendo-se sempre atualizado sobre boas práticas e riscos emergentes em Segurança da Informação;

- **Assinar termos de confidencialidade e adesão às políticas do Sistema de Gestão de Segurança da Informação (SGSI)**, antes de iniciar qualquer atividade, formalizando o compromisso com a segurança da informação;
- **Respeitar os limites de acesso definidos pela TELTEX**, acessando somente sistemas, dados e áreas autorizadas, conforme o escopo do respectivo serviço;
- **Zelar pela segurança dos ativos sob sua responsabilidade,** incluindo servidores, câmeras, softwares, redes e qualquer infraestrutura que operem ou mantenham (ver **POL-03 Política de Uso e Conservação de Equipamentos Teltex**);
- **Reportar falhas técnicas ou riscos identificados**, colaborando com a **Área de Tecnologia da Informação** da **TELTEX** para mitigar vulnerabilidades e evitar incidentes; e
- **Não realizar armazenamento e/ou tratamento indevidos de dados fora dos sistemas autorizados**, não salvando imagens ou informações em dispositivos pessoais ou não homologados.
- **Segurança da informação para uso de serviços em nuvem:** não realizando o compartilhamento de documentos, pastas ou quaisquer dados institucionais por meio de links públicos, ou seja, aqueles em que qualquer pessoa de posse do link pode acessar ou plataformas como OneDrive, GoogleDrive, Dropbox ou similares, sem a devida camada de proteção e controle de acesso. O usuário, caso necessite na atribuição de suas funções dentro da **TELTEX** compartilhar externamente pastas e arquivos, deverá realizar o compartilhamento inserindo o e-mail corporativo do destinatário, permitindo assim gerenciamento posterior e rastreabilidade de acesso.

4.3 Classificação da Informação

Toda informação gerada ou editada como efeito direto ou de suporte da realização dos trabalhos desenvolvidos pela **TELTEX** é considerada seu ATIVO, protegido nos termos da lei. Sua classificação refere-se à categorização dos dados com base em sua sensibilidade e necessidade de proteção. Essa classificação ajuda a definir controles de segurança apropriados para garantir a confidencialidade, integridade e disponibilidade das informações, sendo caracterizada, entre outros, por:

- **Propriedade intelectual:** Criações do intelecto humano, como invenções, marcas, desenhos industriais e obras de hardware e software, cujo conjunto de direitos é reservado pela Lei nº 9.279 de 14/05/1996, a qual regula os direitos e obrigações relativos à propriedade industrial, abrangendo patentes, marcas e repressão à concorrência desleal.
- **Valor estratégico:** Informações sobre clientes, fornecedores, processos e inovação e outras que possam ser essenciais para decisões de negócios.
- **Impacto financeiro:** Dados protegidos que possam gerar vantagem competitiva e evitar prejuízos causados por vazamento ou uso indevido.
- **Regulamentação e conformidade:** Informações protegidas conforme regulamentação vigente e sujeitas à penalidades legais, incluindo mas não se limitando à Lei Federal 13.709 de 14/08/2018 Lei Geral de Proteção de Dados Pessoais (LGPD).
- **Dependência operacional:** Dados internos estruturados que garantam a continuidade dos negócios e a eficiência dos processos.
- **Risco associado:** Informação que se comprometida possa gerar danos à reputação e confiabilidade da empresa.

De forma resumida, as faixas de classificação utilizadas na análise dos riscos de SGSI são:

Nível de Classificação	Classificações correspondentes
1. Normal/rotina:	Dependência operacional; Risco associado
2. Moderado:	Propriedade intelectual; Impacto financeiro
3. Crítico:	Regulamentação e conformidade; Valor estratégico

4.4 Controle de Acesso

Os níveis de acesso às informações (ativos) são categorizados com base na confidencialidade, integridade e disponibilidade. A **TELTEX** adota os seguintes níveis de acesso:

Nível de Acesso	Descrição	Análise
1. Público:	Pode ser acessado por qualquer pessoa.	Informações acessíveis a qualquer pessoa, sem restrições de segurança
2. Interno:	Disponível apenas para funcionários da organização.	Dados destinados apenas a funcionários ou membros da organização, sem acesso externo
3. Restrito:	Acesso limitado a grupos específicos.	Informações sensíveis, acessíveis apenas a grupos específicos dentro da organização
4. Confidencial:	Acesso extremamente restrito.	Dados altamente críticos, acessíveis apenas a indivíduos autorizados, com controles rigorosos

Controles de acesso físico são detalhados na **POL-02 Política de Acesso às Instalações Teltex** à qual estabelece as diretrizes para implementação de medidas para regular a segurança no acesso físico de pessoas aos recursos de processamento, armazenamento e tratamento de dados corporativos de Tecnologia da Informação e Comunicação (TIC) pertencentes à **TELTEX** e aqueles pertencentes à seus clientes que estejam sob seu controle e proteção, de forma a minimizarem os riscos à segurança das informações corporativas.

O acesso lógico é protegido por meio dos Controles Tecnológicos apontados na **FORM-SGSI-06.1.03 Declaração de Aplicabilidade**.

4.4.1 Segurança Física e Ambiental

Os equipamentos de vigilância (câmeras, servidores, DVRs) são adquiridos pela **TELTEX** de fornecedores homologados, e os profissionais designados para sua instalação assinam termos e condições de contratação na forma de instrumentos legais; A responsabilidade sobre a integridade e inviolabilidade destes equipamentos na propriedade do Cliente, entretanto, é de responsabilidade do Cliente.

Em suas dependências, a **TELTEX** utiliza perímetros físicos de segurança (barreiras tais como paredes e portões de entrada controlados) para proteger as áreas que contenham instalações de processamento, armazenamento e tratamento de dados além de controles para minimizar o risco de ameaças físicas potenciais, tais como furto, incêndio, explosivos,

fumaça, água, poeira, vibração, efeitos químicos, interferências com o suprimento de energia elétrica, interferência nas comunicações, radiação eletromagnética e vandalismo.

É mantida área de recepção monitorada pelo pessoal ou outros meios para controlar o acesso físico ao local ou edifício da **TELTEX.**

As instalações físicas são monitoradas por sistemas de vigilância e alarmes de presença por infravermelho para detectar acesso não autorizado ou comportamento suspeito, que podem incluir guardas, alarmes de intrusos, sistemas de videomonitoramento, como de circuito fechado de TV e software de gerenciamento de informações de segurança física, gerenciados internamente ou por um provedor de serviços de monitoramento, conforme apropriado.

4.5 Segurança de Operações e Auditorias

A **TELTEX** assegura que a informação permaneça precisa, completa e confiável por meio da documentação dos procedimentos de operação de seu sistema de gestão da qualidade (SGQ), com certificação de 3ª parte ISO 9001.

Auditorias no âmbito do Sistema de Gestão de Segurança da Informação (**SGSI**) são realizadas periodicamente:

- **Auditoria Interna do SGSI:** visa avaliar se o Sistema de Gestão de Segurança da Informação está funcionando conforme o planejado, atendendo aos requisitos da norma ISO/IEC 27001, às diretrizes internas da **TELTEX**, bem aos requisitos legais e regulatórios;
- **Auditoria de Sistemas:** visa avaliar a eficácia dos controles técnicos de segurança, incluindo firewalls, criptografia, autenticação, controle de acesso, backups, entre outros, bem como avaliar a integridade e confiabilidade dos dados e sistemas, assegurando que as informações monitoradas (como imagens, registros de ocorrências, dados de clientes) estejam protegidas contra alterações indevidas ou perda;
- **Simulações para Identificação de Vulnerabilidades (Testes de Penetração/Pentest):** visa identificar vulnerabilidades reais nos sistemas, redes e aplicações antes que sejam exploradas por agentes maliciosos, simulando ataques cibernéticos para avaliar a eficácia dos controles de segurança existentes e mensurando o impacto potencial de uma invasão, permitindo entender quais dados ou operações poderiam ser comprometidos;
- **Validações Internas de Políticas e Controles em SGSI:** realizada pela **Área de Tecnologia da Informação** da **TELTEX**, sobretudo nos controles tecnológicos apontados na **FORM-SGSI-06.1.03 Declaração de Aplicabilidade**, bem com revisão de acessos e permissões.

4.6 Backup e Recuperação de Dados

A **TELTEX** a fim de assegurar a **continuidade dos negócios** diante de falhas, ataques cibernéticos, erros humanos ou desastres naturais adota as práticas de backup e da recuperação de dados.

Esta medida preventiva visa proteger informações críticas, como registros de monitoramento, dados de clientes e configurações de sistemas, mantendo cópias seguras dos dados, de forma que, mesmo em caso de perda ou corrupção, será possível restaurar as informações e retomar as operações com o mínimo de impacto.

O processo de backup envolve a **cópia periódica dos dados** para um local seguro, que poderá abranger um servidor externo, armazenamento em nuvem ou mídia física, em caráter:

- **Completo:** copia todos os arquivos e dados selecionados — independentemente de terem sido modificados ou não;
- **Incremental:** salva apenas os arquivos que foram modificados ou criados desde o último backup — seja ele completo ou incremental; e/ou
- **Diferencial:** copia todos os arquivos que foram modificados ou criados desde o último backup completo.

A escolha da abordagem depende da criticidade dos dados e da tolerância à perda. Critérios de retenção, criptografia e acesso, garantindo que os backups estejam protegidos contra acessos não autorizados, estão detalhados no **SP.TI.DOC.007 Cópia de Segurança - Backup**.

Com relação à recuperação de dados, ou seja, o processo de restaurar as informações a partir das cópias de segurança ("back-up's") em caso de falha, a **TELTEX** pode utilizar abordagem de forma automatizada ou manual, dependendo da tecnologia utilizada e do nível de confidencialidade dos dados.

O plano de recuperação de dados da **TELTEX** inclui:

- **Validar a integridade do arquivo de backup:** antes de restaurar, é verificado se o arquivo de backup não está corrompido;
- **Processo de restauração:** a **TELTEX** utiliza sistemas (softwares) de gerenciamento de backup para iniciar a restauração;
- **Escolha do destino da recuperação:** definição se os dados serão restaurados no ambiente original ou em um ambiente de testes;
- **Monitoramento do processo e validação dos dados restaurados:** a **Área de Tecnologia da Informação** da **TELTEX** acompanha a restauração dos dados, podendo envolver a área solicitante à qual, ao final, verifica se os dados estão completos, íntegros e funcionais. Isso pode incluir testar sistemas, imagens, registros e acessos.

A **Área de Tecnologia da Informação** da **TELTEX** registra todas as ocorrências de recuperação e restauração no **FORM-SGSI-08.13.01 Registro de Restauração de Dados à partir de Backup**, incluindo o tempo de recuperação (RTO), o ponto de recuperação (RPO) e quaisquer falhas ou melhorias identificadas, fortalecendo o SGSI e preparando a empresa para futuras ocorrências.

4.7 Gestão de Incidentes de Segurança

A **TELTEX** compreende que os incidentes identificados devem ser respondidos conforme sistemáticas padronizadas, conforme **SP.TI.DOC.002 Gestão de Incidentes de Segurança da Informação**, o qual contempla um plano de resposta a incidentes que inclua etapas

específicas para contenção, erradicação e recuperação de incidentes (ver **FORM-SGSI-05.24.01**).

A **TELTEX** avalia eventos de segurança para decidir se eles são incidentes de segurança, de forma que o Sistema de Gestão de Segurança da Informação (SGSI) da **TELTEX** classifique o incidente como:

Classificação	Descrição	Exemplos
• **Menor porte**:	• sem impacto relevante	• **Tentativa de phishing bloqueada:** Um e-mail malicioso é detectado e filtrado pelo sistema antispam antes de chegar ao usuário. • **Acesso negado por erro de autenticação:** Um colaborador tenta acessar um sistema sem permissão, mas o controle de acesso impede. • **Falha pontual de backup secundário:** O backup automático de rotina falha, mas há redundância e nenhum dado é perdido. •
• **Médio porte**:	• impacto limitado e controlável	• **Vazamento de dados internos não sensíveis:** Um relatório interno é compartilhado por engano com terceiros, mas não contém dados pessoais ou estratégicos. • **Malware em estação de trabalho isolada:** Um computador é infectado, mas está fora da rede principal e é rapidamente formatado. • **Interrupção temporária de sistemas de transmissão de dados, incluindo e-mail:** O serviço fica fora do ar por algumas horas, afetando a comunicação, mas sem perda de dados.
• **Grande porte**:	• risco elevado à operação ou à privacidade de dados pessoais	• **Ransomware em rede corporativa:** Sistemas críticos são criptografados, exigindo pagamento para liberação. Operações ficam paralisadas. • **Vazamento de dados pessoais de clientes:** Informações como CPF, endereço e dados bancários são expostas, exigindo notificação à ANPD. • **Comprometimento de credenciais de administrador:** Um invasor obtém acesso privilegiado, podendo alterar configurações e acessar dados confidenciais.

Os incidentes classificados pela área de T.I. da **TELTEX** como grande porte são respondidos conforme procedimentos documentados (ver **FORM-SGSI-05.24.01**), o qual contempla um plano de resposta a incidentes que inclua etapas específicas para:

- Identificação do Incidente
  - Origem do incidente
  - Tipo de incidente
  - Sistemas comprometidos
  - Data e hora da detecção
  - Responsável pela detecção
  - Classificação Inicial
- Descrição
- Detalhamento
  - Vetor de Ataque
  - Origem do acesso
  - Possíveis Ferramentas utilizadas pelo invasor
  - Tempo de exposição
  - Logs de auditoria
- Contenção
  - Revogação das credenciais comprometidas
  - Bloqueio de acesso externo aos sistemas sob controle TELTEX
  - Comunicação aos titulares afetados
  - Notificação à Autoridade Nacional de Proteção de Dados (ANPD) conforme artigo 48 da LGPD
- Avaliação de Impacto
  - Dados comprometidos
  - Risco à privacidade
  - Impacto operacional/ financeiro/ legal
  - Impacto Reputacional
- Análise Forense
  - Análise Técnica Detalhada
  - Determinação da Origem e Vetor de Ataque
  - Documentação e Relatório Forense
- Ações Corretivas de Longo Prazo e Preventivas
  - Análise de Causa Raiz (Root Cause Analysis)
  - Revisão e Atualização de Políticas de Segurança
  - Reforço na Gestão de Vulnerabilidades
  - Melhoria na Arquitetura de Segurança
  - Monitoramento Contínuo e Inteligência de Ameaças
  - Auditorias e Testes Regulares
  - Revisão do Plano de Resposta a Incidentes
- Suporte à Resposta e Recuperação
  - Apoio à equipe de resposta a incidentes (CSIRT)
  - Validação das ações corretivas e restaurativas
  - Monitoramento pós-incidente para garantir que não haja recorrência

4.8 Proteção de Dados Pessoais

A **TELTEX** mantém sua **POL-05 Política de Proteção à Privacidade de Dados Pessoais** disponível à: Colaboradores e prestadores de serviços internos, Prestadores de serviços de TI, Consultorias e auditores externos, Fornecedores de software, Serviços terceirizados com acesso físico ou lógico, Serviços de comunicação e transporte de dados e Serviços jurídicos e contábeis.

4.9 Bases legais para o tratamento de dados pessoais (DP)

A **TELTEX** justifica o tratamento de dados em suas operações com as seguintes bases legais previstas na LGPD:

4.9.1 Cumprimento de obrigação legal ou regulatória

A LGPD, em seu artigo 7º, inciso II, autoriza o tratamento de dados pessoais sem consentimento quando necessário para o cumprimento de obrigação legal ou regulatória pelo controlador.

4.9.2 Execução de contrato

A base legal de execução de contrato (art. 7º, inciso V da LGPD) permite o tratamento de dados pessoais sem consentimento, desde que seja necessário para a execução de um contrato do qual o titular dos dados seja parte ou para procedimentos preliminares relacionados a esse contrato

4.9.3 Exercício regular de direitos

Prevista no art. 7º, inciso VI da LGPD, essa base legal permite o tratamento de dados sem consentimento quando for necessário para:

- Defesa em processos judiciais, administrativos ou arbitrais
- Preservação de provas
- Resguardo do contraditório e da ampla defesa

4.9.4 Proteção da vida ou da incolumidade física

Permite o tratamento de dados sem consentimento quando for necessário para:

"A proteção da vida ou da incolumidade física do titular ou de terceiro."

Ou seja, com o objetivo principal for evitar riscos, prevenir acidentes ou proteger pessoas em ambientes monitorados.

4.9.5 Tutela da saúde

A base legal da tutela da saúde (art. 7º, inciso VIII da LGPD) é voltada principalmente para o tratamento de dados pessoais sensíveis quando necessário para procedimentos realizados por profissionais da saúde, serviços de saúde ou autoridade sanitária; No contexto das atividades da **TELTEX** que realiza vigilância e monitoramento, pode ser invocada caso a empresa esteja envolvida em situações específicas que envolvam risco à saúde ou apoio a serviços médicos, como mas não se limitando à:

- Monitoramento em hospitais, clínicas ou unidades de saúde, onde os sistemas de vigilância apoiam diretamente a proteção de pacientes e profissionais
- Controle de acesso a áreas críticas de saúde, como salas de isolamento ou laboratórios, com uso de biometria ou câmeras
- Resposta a emergências médicas, onde o registro por câmeras pode ser usado para apoiar o atendimento ou investigação de incidentes de saúde

4.10 Obtenção de consentimento

No contexto da prestação de serviços de vigilância e monitoramento, em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) e com os requisitos da norma ISO/IEC 27701, o CLIENTE é o único responsável pela obtenção do consentimento dos titulares dos dados pessoais eventualmente coletados por meio de câmeras de vigilância, sistemas de biometria ou quaisquer outros dispositivos de captação instalados em suas dependências físicas.

NOTA – Tanto as bases legais "Execução de Contrato" quanto a "Obrigação Legal/Regulatória" dispensam o consentimento do titular dos dados pessoais, e se encontram documentadas na presente Política com clareza, incluindo:

- A finalidade específica
- A relação contratual existente
- Os dados tratados
- E os limites do uso, conforme o contrato

4.10.1 Casos aplicáveis para registro do consentimento

4.10.1.1 Monitoramento em áreas privadas ou sensíveis

- **Exemplo:** câmeras em ambientes como vestiários, salas de descanso ou áreas de uso restrito
- **Justificativa:** o tratamento pode afetar diretamente a privacidade do titular, exigindo consentimento explícito

4.10.1.2 Uso de dados para finalidades secundárias

- **Exemplo:** utilizar imagens gravadas para fins de marketing, treinamento interno ou divulgação institucional
- **Justificativa:** essas finalidades não estão diretamente ligadas à execução do contrato ou obrigação legal

4.10.1.3 Tratamento de dados sensíveis sem respaldo legal específico

- **Exemplo:** uso de **biometria** para controle de acesso em locais onde não há exigência legal ou contratual
- **Justificativa:** dados biométricos são sensíveis e exigem consentimento, salvo se houver outra base legal clara

4.10.1.4 Compartilhamento com terceiros fora do escopo contratual

- **Exemplo:** envio de dados para parceiros comerciais, empresas de tecnologia ou plataformas externas
- **Justificativa:** se não houver base legal como execução de contrato ou legítimo interesse, o consentimento é necessário

4.10.1.5 Gravação de áudio em conjunto com vídeo

- **Exemplo:** sistemas de CFTV que capturam som ambiente
- **Justificativa:** o áudio pode revelar informações pessoais não visíveis, exigindo consentimento em alguns contextos

4.11 Política de retenção e descarte de imagens e dados

A retenção e descarte de imagens e informações, podendo incluir dados pessoais (DP) sob controle e tutela da **TELTEX** obedece ao disposto em seu **SP.TI.DOC.004 Exclusão (Descarte) de informações**, o qual estabelece conforme legislação vigente:

- Retenção de Dados;

Titular	Tempo de Retenção	Tipo de Informação	Exemplos comuns em empresas de vigilância
Colaboradores, Prestadores de Serviços	**Durante o vínculo contratual** e, após o desligamento, por:	Dados de identificação	Nome, CPF, RG, endereço, telefone

Titular	Tempo de Retenção	Tipo de Informação	Exemplos comuns em empresas de vigilância
	- 5 anos para fins trabalhistas (ex: ações judiciais, FGTS, INSS) conforme o artigo 7º, inciso XXIX da Constituição Federal. **- 6 anos** para obrigações fiscais, conforme o artigo 173 do Código Tributário Nacional.		
Usuários dos Clientes	**Enquanto forem necessários** para a prestação do serviço de vigilância ou para atender obrigações legais ou contratuais.		
Colaboradores, Prestadores de Serviços	**Durante a vigência do contrato ou prestação de serviço** para garantir segurança, controle de acesso e prestação adequada dos serviços. **Após o término da relação contratual** por até **5 anos**, com base em prazos prescricionais do Código Civil e da legislação trabalhista, caso os dados possam ser úteis em investigações, auditorias ou disputas legais.	Dados de acesso e localização	Horário de entrada/saída, áreas visitadas
		Dados visuais	Imagens de câmeras, vídeos, capturas
		Dados de comportamento	Padrões de movimentação, alertas gerados
		Dados biométricos (se aplicável)	Impressão digital, reconhecimento facial
Usuários dos Clientes	**Enquanto forem necessários** para a prestação do serviço de vigilância ou para atender obrigações legais ou contratuais.	Dados de acesso e localização	Horário de entrada/saída, áreas visitadas
		Dados visuais	Imagens de câmeras, vídeos, capturas
		Dados de comportamento	Padrões de movimentação, alertas gerados

- Exclusão de Informações;
- Métodos de Exclusão;
- Registro dos resultados da exclusão como evidência;
- Descarte Seguro de Mídia.

4.12 Avaliação de impacto de privacidade de dados pessoais (DP)

O **FORM-SGSI-05.34.01Relatório de Impacto à Proteção de Dados Pessoais (RIPD)** é uma exigência prevista na **Lei Geral de Proteção de Dados (LGPD)**, especificamente nos **artigos 5º, inciso XVII, e 38 da Lei nº 13.709/2018**, constituindo uma ferramenta estratégica que ajuda o controlador a **avaliar os riscos** e **documentar as medidas de mitigação** em operações de tratamento de dados que possam representar **alto risco aos direitos e liberdades dos titulares**.

4.13 Aquisição, Desenvolvimento e Manutenção de Sistemas

As diretrizes e critérios referentes às expectativas sobre o comportamento da **TELTEX** e de seus fornecedores estão descritas na **POL-04 Diretrizes de Segurança da Informação para Provedores Externos**, de forma a assegurar o enfrentamento de riscos de segurança associados ao uso de produtos e serviços prestados pelos fornecedores, podendo incluir o acesso físico de pessoas aos recursos de processamento, armazenamento e tratamento de dados corporativos de Tecnologia da Informação e Comunicação (TIC) pertencentes à **TELTEX** e aqueles pertencentes à seus clientes que estejam sob seu controle e proteção.

Desenvolvedores e Programadores assinam o **Termo de Confidencialidade de Acesso ao Código-Fonte**, de forma a assegurar a confidencialidade, integridade e proteção das informações relacionadas ao código fonte de software desenvolvido internamente pela **TELTEX** e as ferramentas de desenvolvimento e bibliotecas de software, conforme os princípios e controles estabelecidos pelas normas ISO/IEC 27001 e ISO/IEC 27002.

Cláusulas adicionais de segurança da informação e privacidade de dados pessoais podem ser especificadas em Contratos.

4.14 Sanções e Penalidades

O descumprimento de qualquer cláusula da presente Política poderá implicar:

- Sanções contratuais específicas, tais como, mas não se limitando à:
  - Advertência com indicação de prazo para adoção de medidas corretivas
  - Multas enquanto durar o descumprimento
  - Denúncia da infração envolvendo incidentes com dados pessoais (DP) à ANPD (Autoridade Nacional de Proteção de Dados), o que pode afetar a reputação da empresa
  - Bloqueio de novos negócios até regularização
- Responsabilização civil e criminal, podendo gerar indenizações por danos materiais e morais;
- Adoção de outras medidas judiciais cabíveis, inclusive legislação trabalhista e fiscal.