Elaboração:	Análise Crítica/Aprovação:	Rev:	Data	Natureza das Alterações
Thales Rollo	Mariana Duardes	00	02/07/2025	Versão inicial

1. Apresentação

A **TELTEX TECNOLOGIA S.A,** vem por meio desta política estabelecer as diretrizes e critérios referentes às expectativas sobre o nosso comportamento e de nossos fornecedores de forma a enfrentar 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.

Estas diretrizes devem ser lidas, compreendidas e seguidas pelos 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 provedores externos:

- **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 (1º andar)
  - Showroom (1º andar)
  - Sala Técnica (1º 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.

3. Público alvo

Estas diretrizes se aplicam a todos os fornecedores, 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.

A presente Política busca atingir em especial o seguinte público:
- Fornecedores
- Prestadores de serviço

4. Procedimento

4.1 As atividades de Compras da **TELTEX** compreendem a organização da cadeia de suprimentos que agrega valor ao adquirir produtos e serviços de forma estratégica, por meio de processos de compras uniformes e confiáveis, e ao garantir que tais produtos ou serviços sejam entregues ou prestados às operações da **TELTEX**.

4.2 Os Agentes de Compras da **TELTEX** são os principais operadores na cadeia de suprimentos recebidos para todas as suas operações, e interagem com os fornecedores de acordo com os princípios básicos de respeito e integridade.

4.3 A presente política tem efeitos de acordo documentado com os fornecedores da **TELTEX** para assegurar que haja um entendimento claro entre a organização e o fornecedor sobre as obrigações de ambas as partes de cumprir com os requisitos relevantes de segurança da informação.

5. Generalidades

5.1 A **TELTEX** identifica e documenta os tipos de fornecedores (por exemplo, serviços de TIC, logística, utilidades, serviços financeiros, componentes de infraestrutura de TIC) que podem afetar a confidencialidade, integridade e disponibilidade das informações da organização por meio de seu **FORM-SGSI-05.19.01 Controle de Fornecedores com Riscos Associados à Segurança da Informação**;
Neste formulário são identificados:
- Fornecedor e CNPJ;
- Tipo de Fornecedor:
  - 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
  - Serviços jurídicos e contábeis
- Produto ou Serviço;
- Nível de acesso ao Local:
  - Recepção (1º andar)
  - Showroom (1º andar)
  - Sala Técnica (1º andar)
  - Sala Administrativa (2º andar)
  - Sala Comercial e CPD (3º andar)
- Nível de acesso à informação (rede/software):

- Administrador
- Usuário
- Código fonte
- Não Aplicável

- Riscos identificados
- Controles aplicados
- Situação em relação ao aceite das diretrizes da presente Política

5.2 Os provedores externos para os quais foram identificados riscos associados à Segurança da Informação devem assinar e retornar à **TELTEX** o **FORM-SGSI-05.19.02 Termo de Aceite e Compromisso do Provedor Externo com as Políticas de SGSI**. Este termo celebrado entre as partes formaliza o comprometimento do fornecedor com as diretrizes de segurança da informação da **TELTEX,** garantindo legalmente que terceiros que tenham acesso a dados, sistemas ou infraestrutura crítica estejam alinhados com os mesmos padrões de proteção e conformidade.

5.2.1 O provedor externo (ou fornecedor) se compromete por meio da presente política à atender à todos os requisitos legais, estatutários, regulamentares e contratuais, incluindo proteção de dados, manuseio de dados pessoais (DP), direitos de propriedade intelectual e direitos autorais implicados no fornecimento de seus produtos e/ou serviços à **TELTEX**.

5.3 A **TELTEX** avalia e seleciona fornecedores de acordo com a sensibilidade de informações, produtos e serviços (por exemplo, com análise de mercado, referências ao cliente, análise crítica de documentos, avaliações no local, certificações);

5.4 A **TELTEX** também avalia e seleciona produtos ou serviços do fornecedor que tenham controles adequados de segurança da informação e procura analisá-los criticamente sempre que necessário; em particular, a precisão e a completeza dos controles implementados pelo fornecedor que assegure a integridade do tratamento de informações e informações do fornecedor e, consequentemente, a segurança da informação da **TELTEX**, no caso de fornecedores considerados críticos e/ou estratégicos, em especial quando incluírem tipos de componentes e serviços de infraestrutura de TIC fornecidos pelos fornecedores que possam afetar a confidencialidade, integridade e disponibilidade das informações da **TELTEX** e de seus clientes.

5.5 No **FORM-SGSI-05.19.01 Controle de Fornecedores com Riscos Associados à Segurança da Informação** estão estabelecidas as informações da **TELTEX**, os serviços de TIC e a infraestrutura física que os fornecedores podem acessar, monitorar, controlar ou usar.

5.6 Os riscos de segurança da informação associados:

5.6.1 ao uso das informações da **TELTEX** pelos fornecedores e outros ativos associados, incluindo riscos originários de potenciais fornecedores maliciosos;

5.6.2 ao mau funcionamento ou vulnerabilidades dos produtos (incluindo componentes de software e subcomponentes utilizados nesses produtos) ou serviços prestados pelos fornecedores;

são avaliados e gerenciados por meio do **FORM-SGSI-06.1.02 Análise, Avaliação e Tratamento de Riscos de SGSI**, incluindo monitoramento de compliance com os requisitos estabelecidos de segurança da informação para fornecedores considerados críticos e/ou

estratégicos, podendo ainda haver análise crítica e validação do produto pela equipe de Tecnologia da Informação da **TELTEX** ou por terceiros, conforme cada caso.

5.7 A **TELTEX** determina controles e os aplica para gerenciar o acesso do fornecedor às informações e outros ativos associados, para que suas informações e as informações de suas Partes Interessadas sob sua guarda ou tutela não sejam colocadas em risco por fornecedores com uma gestão inadequada de segurança da informação. Estes riscos podem ser causados por controles inadequados de componentes de infraestrutura de TIC ou serviços prestados pelos fornecedores; Componentes ou serviços defeituosos ou vulneráveis podem causar violações de segurança da informação na organização ou em outra entidade (por exemplo, eles podem causar infecção por malware, ataques ou outros danos a entidades que não a organização).

5.7.1 Cada parte contratual, os provedores externos (fornecedores) e **TELTEX** se obrigam pela presente política a implementar um conjunto de controles acordados, incluindo controle de acesso, análise crítica de desempenho, monitoramento, relatos e auditorias, para os riscos considerados críticos; O fornecedor se compromete em estar em conformidade com os requisitos de segurança da informação da **TELTEX**.

5.8 Incidentes e contingências associados a produtos e serviços de fornecedores, incluindo responsabilidades tanto da **TELTEX** quanto dos fornecedores, serão investigados por nosso time Tecnologia da Informação, podendo envolver empresas especializadas conforme o caso, para o que se espera inteira cooperação do provedor externo envolvido. O provedor externo ("fornecedor") se encontra obrigado ainda à comunicar à **TELTEX**, em prazo máximo de 24 horas úteis, qualquer incidente de segurança, falha ou vazamento que envolva informações sob sua guarda ou tutela (ver "Gestão de Incidentes de Segurança da Informação" na presente política).

5.8.1 Conforme o nível de criticidade do produto e/ou serviço provido pelo fornecedor, pode ser exigida garantia da disponibilidade de uma instalação alternativa (por exemplo, local de recuperação de desastres) não sujeita às mesmas ameaças que a instalação primária e considerações de controles de retorno (controles alternativos), caso os controles primários falhem.

5.9 O fornecedor deve possuir uma sistemática definida para gestão de mudanças que assegure a notificação prévia à **TELTEX** e a possibilidade dela de não aceitar alterações no disposto na presente política, Objeto do Contrato ou Acordo; Estas mudanças podem incluir o seguinte:

- melhorias nos serviços atuais oferecidos;
- desenvolvimento de quaisquer novas aplicações e sistemas;
- modificações ou atualizações das políticas e procedimentos do fornecedor;
- controles novos ou alterados para resolver incidentes de segurança da informação e melhorar a segurança da informação;
- mudanças e aprimoramento das redes;
- uso de novas tecnologias;
- adoção de novos produtos ou versões ou lançamentos mais recentes;
- novas ferramentas e ambientes de desenvolvimento;
- alterações na localização física das instalações de serviço;
- mudança de subfornecedores;
- subcontratação de outro fornecedor; entre outras.

5.10 A **TELTEX** pode considerar os procedimentos para o tratamento contínuo de informações, caso o fornecedor não consiga fornecer seus produtos ou serviços (por exemplo, por causa de um incidente, pois o fornecedor não está mais no negócio, ou não fornece mais alguns componentes devido aos avanços tecnológicos), para evitar qualquer atraso na organização de produtos ou serviços de substituição (por exemplo, identificando um fornecedor alternativo com antecedência ou sempre usando fornecedores alternativos).

5.10.1 Independentemente disso, o fornecedor deve manter a capacidade de serviço suficiente, juntamente com planos viáveis projetados para assegurar que os níveis de continuidade de serviço acordados sejam mantidos após grandes falhas de serviço ou desastre.

5.11 A **TELTEX** espera que seus fornecedores apliquem resiliência e, se necessário, medidas de recuperação e contingência para assegurar a disponibilidade do tratamento de suas informações e/ou de informações sob a guarda ou tutela do fornecedor e, consequentemente, a disponibilidade das informações da **TELTEX** e/ou de seus clientes para o seu uso pretendido nos prazos acordados em contrato.

5.11.1 Para os fornecedores considerados críticos, podem ser solicitados mecanismos de evidência e garantia de atestados de terceiros para requisitos relevantes de segurança da informação relacionados aos processos de fornecedores e um relatório independente sobre a eficácia dos controles, bem como o direito de auditar os processos e controles do fornecedor relacionados ao acordo de fornecimento.

5.12 A transferência necessária de informações, outros ativos associados e qualquer outra coisa que precise ser alterada deve ser gerenciada pelo fornecedor de forma a assegurar que a segurança da informação seja mantida durante todo o período de transferência.

5.12.1 Conforme o nível de criticidade do produto e/ou serviço provido pelo fornecedor, controles de transferência de informações para proteger as informações durante a transferência física ou transmissão lógica podem ser exigidos.

5.13 O fornecedor deve ainda conscientizar e treinar seu pessoal na interação com o pessoal da **TELTEX** sobre as regras nesta política e/ou outras regras estabelecidas em contrato, buscando o engajamento no atendimento às políticas específicas por tema para processos e procedimentos e comportamentos baseados no tipo de fornecedor e no nível de acesso do fornecedor aos sistemas de informações da **TELTEX**. A aplicação de tais regras tem por objetivo assegurar a confidencialidade, integridade e disponibilidade das informações da **TELTEX** e de suas partes interessadas.

5.13.1 O fornecedor deve obedecer e transmitir as disposições relevantes com a presente política para a subcontratação, incluindo os controles que precisam ser implementados por exemplo, exigindo tê-los sob as mesmas obrigações do próprio fornecedor.

6. Informações Fornecidas ou Acessadas por Fornecedores e Teltex

6.1 As informações a serem fornecidas ou acessadas e métodos de fornecimento ou acesso à estas informações estão descritas no **Objeto de Contrato** celebrado entre as partes e cláusulas complementares.

6.2 O provedor externo (fornecedor) se compromete a utilizar as informações da **TELTEX** e/ou de suas Partes Interessadas fornecidas ou acessadas por ele conforme regras de uso

aceitável de informações e outros ativos associados, incluindo uso inaceitável, se necessário:

6.2.1 Uso aceitável das informações da **TELTEX** e/ou de suas Partes Interessadas fornecidas ou acessadas pelo fornecedor:

- Uso conforme contrato ou acordo: As informações só podem ser utilizadas para os fins definidos nos contratos, acordos de confidencialidade (NDA) ou termos de serviço.

- Proteção contra acesso não autorizado: O fornecedor deve implementar controles para garantir que apenas pessoas autorizadas tenham acesso às informações.

- Proibição de compartilhamento indevido: É vedado o repasse de dados a terceiros sem autorização expressa da organização.

- Retenção e descarte seguro: As informações devem ser armazenadas pelo tempo necessário e descartadas de forma segura após o término do contrato ou projeto.

- Conformidade com leis e normas: O uso deve estar alinhado com legislações como a LGPD (Lei Geral de Proteção de Dados) e normas como a ISO/IEC 27001.

- Responsabilidade por incidentes: O fornecedor deve comunicar imediatamente qualquer incidente de segurança relacionado às informações acessadas.

6.2.2 Uso inaceitável das informações da **TELTEX** e/ou de suas Partes Interessadas fornecidas ou acessadas pelo fornecedor:

- Compartilhamento não autorizado: Divulgar informações da organização ou de suas partes interessadas a terceiros sem consentimento formal.

- Uso para fins pessoais ou comerciais: Utilizar dados obtidos para benefício próprio ou para outras atividades que não estejam previstas no contrato.

- Armazenamento inseguro: Manter informações em dispositivos ou ambientes sem proteção adequada contra acesso indevido.

- Modificação ou manipulação indevida: Alterar dados sem autorização ou fora dos processos estabelecidos.

- Retenção indevida após o término do contrato: Manter informações além do período permitido, sem justificativa legal ou contratual.

- Violação de leis e normas: Descumprir legislações como a LGPD ou requisitos da ISO/IEC 27001, colocando em risco a **TELTEX** e suas Partes Interessadas.

6.2.3 O fornecedor se compromete seguir os procedimentos ou condições para autorização e remoção da autorização para uso das informações da **TELTEX** e suas Partes Interessadas e outros ativos associados acessados por pessoal do fornecedor conforme informado pelas Políticas de Segurança da Informação da **TELTEX** devendo procurar a área de Sistema de Gestão de Segurança da Informação (SGSI) da **TELTEX** no e-mail ti@teltex.com.br para eventual esclarecimento.

6.2.4 Os requisitos mínimos de segurança da informação em relação à infraestrutura física de Tecnologia da Informação e Comunicação (TIC) do fornecedor e/ou aos produtos de hardware fornecidos por este e/ou associados à sua prestação de serviço, em particular os requisitos mínimos de segurança da informação para cada tipo de informação e tipo de acesso para servir de base para acordos individuais de fornecedores com base nas necessidades de negócio e critérios de risco da **TELTEX** estão definidos na presente política e de forma complementar no Objeto de Contrato ou Acordo com cada fornecedor.

7. Classificação das Informações e Teltex

7.1 A fim de assegurar que cada dado ou informação receba o nível adequado de proteção, a **TELTEX** classifica as informações de acordo com o esquema de classificação á seguir:

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

7.1.1 Caso o fornecedor identifique fatores absolutamente incompatíveis entre o esquema de classificação da **TELTEX** e o seu próprio esquema de classificação, deve procurar a área de Sistema de Gestão de Segurança da Informação (SGSI) da **TELTEX** no e-mail ti@teltex.com.br para eventual alinhamento.

8. Acesso às Instalações da Teltex

8.1 A fim de assegurar um nível adequado de segurança pessoal e segurança física esperado do pessoal do fornecedor, os critérios definidos na **Política de Acesso às Instalações da Teltex** deverão ser observados enquanto sua presença se fizer necessária para qualquer tipo de prestação de serviço e/ou entrega de produto. Atalho seguro para a versão vigente desta política está disponível em nosso website https://teltex.com.br.

9. Uso Responsável de dispositivos eletrônicos de propriedade da TELTEX

9.1 A **TELTEX** disponibiliza equipamentos eletrônicos para colaboradores e/ou prestadores de serviço, nos níveis organizacionais pertinentes, para utilização única e exclusiva a serviço da empresa tendo em vista a atividade a ser exercida pelo usuário, o qual tem somente a detenção provisória do equipamento eletrônico/dispositivo (que é de propriedade da **TELTEX**), tendo em vista o uso exclusivo para prestação de serviços profissionais, não implicando de forma alguma na propriedade do referido equipamento, sendo terminantemente proibidos o empréstimo, aluguel ou cessão deste a terceiros pelo usuário.

9.2 Ao término da prestação de serviço ou do contrato de trabalho, o usuário deve devolver o equipamento eletrônico/dispositivo em perfeito estado no mesmo dia em que for

comunicado ou que comunique seu desligamento ou rescisão do contrato de prestação de serviços.

9.3 Os critérios para uso responsável de dispositivos eletrônicos de propriedade da **TELTEX** estão definidos na Política de Uso e Conservação de Equipamentos Teltex, para a qual é mantido atalho seguro para a versão vigente desta política está disponível em nosso website https://teltex.com.br.

10. Gestão da segurança da informação na cadeia de fornecimento de TIC

10.1 Além dos requisitos gerais de segurança da informação para as relações com fornecedores, outros tópicos podem ser considerados para abordar a segurança da informação dentro da segurança da cadeia de fornecimento de Tecnologia da Informação e Comunicação (TIC), podendo incluir requisitos complementares para a aquisição de produtos ou serviços de TIC, tais como mas não se limitando à:
- histórico de incidentes ou não conformidades notificados à TELTEX e/ou ANPD;
- responsabilidade solidária conforme LGPD;
- adoção de práticas baseadas na ISO 27001;
- controle de acesso baseado em função;
- utilização de criptografia para dados em trânsito e em repouso;
- manutenção de plano próprio de resposta a incidentes de segurança da informação;
- manutenção de canal para comunicação de falhas ou suspeitas.

10.2 Os fornecedores de serviços de TIC devem propagar os requisitos de segurança da **TELTEX** pela cadeia de fornecimento, conforme apropriado, se subcontratarem partes do serviço de TIC prestados à **TELTEX**.

10.3 Os fornecedores de produtos de TIC devem propagar práticas de segurança adequadas pela cadeia de fornecimento, conforme apropriado, se esses produtos incluírem componentes comprados ou adquiridos de outros fornecedores ou outras entidades (por exemplo, desenvolvedores de software subcontratados e provedores de componentes de hardware).

10.4 A **TELTEX** pode, conforme apropriado, solicitar que os fornecedores de produtos de TIC forneçam informações descrevendo as funções de segurança implementadas em seus produtos e as configurações necessárias para a sua operação segura.

10.5 Os fornecedores de TIC devem assegurar como apropriado que os seus componentes sejam genuínos e sem alteração de sua especificação.

10.6 Os fornecedores de TIC devem, conforme apropriado, realizar a gestão do ciclo de vida dos componentes de TIC e disponibilidade e riscos de segurança associados considerando a destruição segura de hardware e componentes bem como a eliminação segura de informações e outros ativos associados desnecessários quando do encerramento do relacionamento profissional com a **TELTEX**.

10.7 As cadeias de fornecimento de TIC, conforme abordado por esta política, incluem serviços em nuvem. Exemplos de cadeias de fornecimento de TIC são:

a) provisão de serviços em nuvem, onde o provedor de serviços em nuvem confia nos desenvolvedores de software, provedores de serviços de telecomunicações, provedores de hardware;
b) IoT, onde o serviço envolve os fabricantes de dispositivos, os provedores de serviços em nuvem (por exemplo, os operadores de plataforma de IoT), os desenvolvedores de aplicações móveis e web, o fornecedor de bibliotecas de software;
c) serviços de hospedagem, onde o provedor conta com service desks externos, incluindo primeiro, segundo e terceiro níveis de apoio.

11. Segurança da informação para uso de serviços em nuvem

11.1 O uso de serviços em nuvem pode envolver responsabilidade compartilhada pela segurança da informação e esforço colaborativo entre o provedor de serviços em nuvem e a **TELTEX**, a qual atua como cliente do serviço em nuvem. As responsabilidades tanto para o provedor de serviços em nuvem quanto para a **TELTEX** estão definidas em Contrato ou Acordo de Serviço celebrado adequadamente entre as partes.

Importante: Os contratos de serviços em nuvem são muitas vezes predefinidos e não estão abertos à negociação, por isso os procedimentos adotados para o tratamento de incidentes de segurança da informação que ocorrerem em relação ao uso de serviços em nuvem podem obedecer ao disposto nas políticas e diretrizes do prestador de serviços em nuvem, uma vez que os mesmos abordam os requisitos de confidencialidade, integridade, disponibilidade e manuseio de informações do cliente do serviço, com objetivos apropriados de nível de serviço em nuvem.

11.2 Os serviços em nuvem provêm o backup necessário de dados e informações de configuração, gerenciando os backups com segurança conforme aplicável, com base nos recursos do provedor de serviços em nuvem usado pela **TELTEX**.

11.3 Convém que os serviços em nuvem comuniquem à TELTEX alterações relevantes quanto à:
a) alterações na infraestrutura técnica (por exemplo, realocação, reconfiguração ou alterações no hardware ou software) que afetem ou alterem a oferta do serviço em nuvem;
b) tratamento ou armazenamento de informações em uma nova jurisdição geográfica ou legal;
c) uso de provedores de serviços em nuvem por pares ou outros subcontratados (incluindo alterar partes existentes ou usar novas partes).

12. Gestão de Incidentes de Segurança da Informação

12.1 A fim de assegurar um nível adequado de segurança da informação, o provedor externo (fornecedor) se compromete em cumprir com os critérios definidos na **SP.TI.DOC.002 Gestão de Incidentes de Segurança da Informação**, devendo para tanto procurar a área de Sistema de Gestão de Segurança da Informação (SGSI) da **TELTEX** no e-mail ti@teltex.com.br para notificação de incidentes e alinhamento em relação às providências necessárias, tais como mas não se limitando à:

12.1.1 Identificação e Detecção

- Monitorar sistemas e redes

- Reconhecer sinais de anomalias ou falhas
- Registrar evidências do incidente

12.1.2 Notificação e Comunicação

- Informar imediatamente os responsáveis na **TELTEX** (ti@teltex.com.br)
- Acionar fornecedores ou terceiros envolvidos
- Comunicar autoridades reguladoras (ex: ANPD), se necessário

12.1.3 Classificação e Avaliação

- Determinar o tipo e gravidade do incidente
- Avaliar impacto nos ativos de informação e na operação
- Priorizar resposta conforme criticidade

12.1.4 Resposta e Contenção

- Isolar sistemas afetados para evitar propagação
- Aplicar medidas emergenciais de segurança
- Preservar evidências para investigação

12.1.5 Remediação e Recuperação

- Corrigir vulnerabilidades exploradas
- Restaurar serviços e dados afetados
- Validar integridade dos sistemas após correção

12.1.6 Registro e Documentação

- Elaborar relatório técnico do incidente
- Registrar ações tomadas e responsáveis envolvidos
- Atualizar base de conhecimento para referência futura

12.1.7 Aprendizado e Melhoria Contínua

- Realizar análise de causa raiz
- Revisar políticas e controles de segurança
- Promover treinamentos e conscientização

12.1.8 Quando um incidente de segurança da informação ocorre por negligência de um fornecedor, a **TELTEX** pode adotar diversas medidas legais e contratuais para proteger seus interesses e garantir responsabilização, conforme a LGPD (Lei 13.709/2018) e princípios da responsabilidade civil, incluindo mas não se limitando às seguintes disposições legais e ações possíveis:

12.1.8.1 Ação de reparação de danos

A **TELTEX** pode exigir indenização por perdas e danos materiais e morais, especialmente se houver prejuízo financeiro ou impacto à reputação.

12.1.8.2 Responsabilidade solidária

Conforme a LGPD, o fornecedor (como operador) pode ser responsabilizado solidariamente com o controlador, caso o incidente afete dados pessoais e haja falha no cumprimento das obrigações legais.

12.1.8.3 Rescisão contratual por descumprimento

Se houver cláusulas de segurança da informação no contrato, a negligência pode justificar a rescisão unilateral e aplicação de penalidades previstas.

12.1.8.4 Notificação à ANPD

A **TELTEX** deve comunicar o incidente à Autoridade Nacional de Proteção de Dados (ANPD), e pode incluir no relatório a conduta negligente do fornecedor.

12.1.8.5 Ação judicial por violação contratual

Caso não haja acordo extrajudicial, a empresa pode ingressar com ação judicial por violação de cláusulas contratuais, especialmente se houver omissão ou demora na comunicação do incidente.

12.1.8.6 Cláusulas de auditoria e compliance

A **TELTEX** pode exigir auditoria nos sistemas do fornecedor e revisão dos controles de segurança, com base em cláusulas contratuais ou políticas internas.

12.1.8.7 Suspensão ou bloqueio de acesso

Como medida preventiva, o fornecedor pode ter seus acessos suspensos até que os riscos sejam mitigados e a conformidade restabelecida.

Importante: A LGPD exige que o operador (fornecedor) colabore com o controlador na resposta ao incidente. A omissão pode agravar sua responsabilidade e comprometer a relação comercial.

13. Monitoramento, análise crítica e gestão de mudanças dos serviços de fornecedores

13.1 A **TELTEX** realiza monitoramento, análise crítica periódica e, quando necessário, gestão de mudanças dos serviços de fornecedores para que assegurem que os termos e condições de segurança da informação da presente política e outras políticas de segurança da informação relacionadas estejam conformes; Além disso, incidentes de segurança da informação e problemas serão gerenciados adequadamente para que mudanças nos serviços de fornecedores ou status de empresa não afetem a prestação de serviços.

14. Encerramento do Relacionamento Profissional

14.1 A **TELTEX** busca assegurar um término seguro do relacionamento com o fornecedor, da seguinte forma:

- desprovisionamento dos direitos de acesso;
- tratamento de informações;
- determinação da propriedade intelectual desenvolvida durante o engajamento;
- portabilidade de informações em caso de alteração de fornecedor ou internalização;
- gerenciamento de registros;
- devolução de ativos;
- eliminação segura de informações e outros ativos associados;
- aplicação de requisitos de confidencialidade em andamento; entre outras.

O provedor externo (ou "fornecedor") deve estar preparado para cooperar em uma ou mais destas maneiras para assegurar um encerramento do relacionamento profissional de forma segura para ambas as partes.

14.2 Conforme o nível de criticidade do produto e/ou serviço provido pelo fornecedor, cláusulas de rescisão após a celebração do contrato, incluindo gerenciamento de registros, devolução de ativos, descarte seguro de informações e outros ativos associados e quaisquer obrigações de confidencialidade em curso podem ser solicitadas pela **TELTEX**, podendo incluir ainda mas não se limitando à provisão de um método de destruição segura das informações da **TELTEX** e suas Partes Interessadas armazenadas pelo fornecedor assim que não forem mais necessárias.