Elaboração:	Análise Crítica/Aprovação:	Rev:	Data	Natureza das Alterações
Ivan Lima	Thales Rollo	00	07/07/2025	Versão inicial

1. Apresentação

O presente documento visa estabelecer diretrizes para identificação, notificação, tratamento e remediação de incidentes de segurança da informação, garantindo conformidade com a ISO 27001 e LGPD.

A **TELTEX** compreende que os incidentes identificados devem ser respondidos conforme sistemáticas padronizadas, conforme o presente documento, 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**).

2. Escopo para Aplicação

Aplica-se a todos os colaboradores, fornecedores e partes interessadas que tenham acesso a ativos de informação da organização, no âmbito do Sistema de Gestão de Segurança da Informação (SGSI) da **TELTEX TECNOLOGIA S.A.**

2.1 Definições Importantes

- **Incidente de Segurança:** Evento que compromete a confidencialidade, integridade ou disponibilidade da informação.
- **Fragilidade:** Vulnerabilidade identificada que pode resultar em incidente.
- **Notificação:** Comunicação formal de um incidente ou fragilidade.
- **Remediação:** Ações corretivas para eliminar ou mitigar os impactos do incidente.

3. Público Alvo

O presente documento busca atingir em especial o seguinte público:

- Colaboradores da área de Tecnologia da Informação responsáveis pela gestão de ativos lógicos da **TELTEX**
- **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.

4. Procedimento

4.1 Planejamento para Gestão de Incidentes de Segurança da Informação (5.24):

A **TELTEX** prepara e testa planos para lidar com incidentes de segurança, estabelecendo claramente responsabilidades e procedimentos.

Pentest, ou teste de penetração, (prática segurança da informação que consiste em simular ataques reais a sistemas, redes ou aplicações para identificar vulnerabilidades antes que sejam exploradas por hackers mal-intencionados) são realizados por meio do provedor externo Gruppen (https://www.gruppen.com.br/solucoes/#solucao-pentest), o qual:

- Identifica de forma proativa vulnerabilidades em sistemas, redes e aplicações;
- Simula ataques reais para avaliar a resiliência do ambiente digital da **TELTEX**;
- Envia relatórios detalhados com recomendações práticas para mitigação de riscos, elaborados por especialistas certificados com experiência em segurança cibernética.

O objetivo destas simulações é testar a capacidade de resposta da organização e atualizar os planos com base nos resultados.

4.2 Identificação de Incidentes

Qualquer colaborador ou fornecedor pode e deve **reportar imediatamente** incidentes ou fragilidades observadas por meio do e-mail especificado

ti@teltex.com.br

A notificação deve conter pelo menos:

- Data e hora do ocorrido
- Descrição do evento
- Ativos envolvidos
- Impacto percebido

4.3 Classificação do Incidente

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.

Classificação	Descrição	Exemplos
		• **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.

4.4 Resposta a Incidentes de Segurança da Informação

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

4.5 Coleta de Evidências

Os procedimentos para identificação, coleta, aquisição e preservação de evidências relacionadas a eventos de segurança da informação estão descritos no **FORM-SGSI-05.24.01 Relatório de Incidentes de Segurança da Informação**, contemplando:

  - Preservação do Ambiente e das Evidências
  - Identificação e Coleta de Evidências

4.6 Colaboração na Remediação

A **TELTEX** espera que equipes técnicas e jurídicas atuem em conjunto; Fornecedores envolvidos devem colaborar conforme cláusulas contratuais e **POL-04 Diretrizes de Segurança da Informação para Provedores Externos**.
Ações incluem:

- Isolamento de sistemas afetados
- Recuperação de dados

- Comunicação com titulares de dados (conforme aplicável)
- Notificação à ANPD (Autoridade Nacional de Proteção de Dados), conforme artigo 48 da LGPD

4.7 Segurança da Informação Durante a Disrupção

A **TELTEX** planeja junto à fornecedores e prestadores de serviço (conforme o caso) como manter a segurança da informação em um nível apropriado durante a disrupção. Isto pode envolver:

A. Isolamento e Contenção Segura
- Impedir a propagação do incidente.
- Preservar a integridade dos sistemas não afetados.

B. Preservação de Evidências Digitais
- Garantir que logs, arquivos e imagens de disco sejam preservados para análise forense.

C. Comunicação Controlada e Segura
- Utilização de canais seguros para comunicação interna.
- Evitar vazamentos de informações sensíveis.

D. Priorização de Ativos Críticos
- Identificar os sistemas essenciais à operação e à proteção de dados pessoais.

E. Aplicação de Controles Temporários
- Reforçar controles de acesso, autenticação e monitoramento.

F. Monitoramento em Tempo Real
- Onde aplicável, ativar ferramentas de SIEM (Security Information and Event Management) e alertas para detectar novas tentativas de ataque.

G. Engajamento da Alta Direção e Jurídico
- Manter a liderança informada para decisões estratégicas e legais.

H. Gestão de Continuidade de Negócios
- Aplicar etapas para continuidade para manter serviços essenciais:
  - Ativação de Ambientes Alternativos
    - Redirecionar operações para ambientes de contingência (ex: servidores de backup, cloud segura).
    - Garantir que os dados estejam íntegros e atualizados (RPO – Recovery Point Objective).
  - Comunicação Estratégica
    - Informar partes interessadas internas e externas, conforme o caso, com transparência e controle.
    - Utilizar canais seguros para evitar vazamentos ou desinformação.
  - Execução de Procedimentos de Recuperação
    - Seguir os procedimentos técnicos para restaurar sistemas e dados.

- Priorizar serviços essenciais como ERP, CRM, Engenharia, e sistemas financeiros

- Monitoramento Contínuo e Reforço de Controles
  - Intensificar o monitoramento de segurança durante o período de recuperação.
  - Aplicar controles adicionais como autenticação multifator e restrição de acessos.

NOTA A prontidão de TIC (ferramentas de Tecnologia da Informação e Comunicação) deve ser mantida com base nos objetivos de continuidade de negócios (ver auditoria de sistemas e auditoria de SGSI).

4.8 Registro e Aprendizado

A **TELTEX** documenta formalmente os incidentes de grande porte por meio do relatório técnico **FORM-SGSI-05.24.01 Relatório de Incidentes de Segurança da Informação** de forma a permitir realizar análise de causa raiz e propor melhorias.

O conhecimento adquirido com incidentes passados é utilizado pela **TELTEX** para fortalecer os controles de segurança.

4.9 Responsabilidades

Função	Responsabilidade
Colaboradores	Reportar incidentes imediatamente
Tecnologia da Informação TELTEX	Classificar, coordenar resposta e remediação
Jurídico/Compliance TELTEX	Avaliar impacto legal e comunicar autoridades
Tecnologia da Informação TELTEX	Executar ações técnicas de contenção e correção
Fornecedores/Prestadores de Serviço	Cooperar conforme acordos e políticas vigentes