Tribunal Regional Eleitoral
do Espírito Santo

Sede: Vitória/ES
Av. João Batista Parra, 575
Praia do Suá - Vitória - ES
CEP 29052-123
Tel.: (27) 2121.8500
Endereço eletrônico:
www.tre-es.jus.br

Comissão de Segurança da Informação

NSI-014	V1.0 - MAR 2025	SEGURANÇA DA INFORMAÇÃO

Gestão de incidentes de segurança da informação

Referência(s):

Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)

Resolução CNJ 396/2021 – ENSEC-PJ

Resolução TSE 23.644/2021 – PSI/JE

Resolução TSE 23.650/2021 – Política Geral de Privacidade e Proteção de Dados Pessoais

Portaria DG/TSE 444/2021, instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral

ABNT ISO/IEC 27001 e ABNT NBR ISO/IEC 27002

ABNT ISO/IEC 27035(1,2 e 3)

Boas práticas de resposta à incidentes previstas no guia NIST SP-800-61 rev.2

Palavras Chave: segurança, norma, incidente | 9 páginas

1. Prefácio

A presente norma está alinhada às diretrizes de Segurança da Informação e dos Dados Pessoais estabelecidas na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) e integra a Política de Segurança da Informação da Justiça Eleitoral (PSI-JE).

2. Objetivo

Estabelecer as principais estratégias no tratamento de incidentes computacionais, que envolvam ou não dados pessoais, permitindo a adequada preparação, detecção, contenção, erradicação, recuperação, avaliação e comunicação destes incidentes.

3. Abrangência

Essa norma se aplica a todos os incidentes de segurança que afetem os ativos de informação do Tribunal, estejam eles na infraestrutura da rede de dados local ou em nuvem.

4. Das definições

4.1. Para efeitos desta norma consideram-se os termos e definições previstos na portaria DG/TSE 444/2021, além dos seguintes:

4.1.1. ANPD – Agência Nacional de Proteção de Dados Pessoais. Órgão da administração pública nacional responsável por fiscalizar e zelar pelo cumprimento da Lei Geral de Proteção de Dados em todo o território brasileiro

4.1.2. CTIR GOV – Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo.

4.1.3. ETIR (Equipe Técnica de Respostas a Incidentes de Segurança Cibernética) – Equipe de tecnologia da informação, de constituição multidisciplinar, coordenada por um Agente Responsável.

4.1.4. Evento de segurança da informação: Alguma mudança de estado em algum ativo ou serviço de TI, como troca de uma senha, log de acesso a um serviço web, bloqueio da execução de um aplicativo pelo antivírus etc.

4.1.5. Incidente de segurança da informação: Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de informação ou das redes de computadores.

4.1.6. Incidente de segurança da informação com dados pessoais: Qualquer incidente de segurança à proteção de dados pessoais, sendo acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou qualquer forma de tratamento de dados ilícita ou inadequada, que tem a capacidade de pôr em risco os direitos e as liberdades dos titulares dos dados pessoais.

4.1.7. Incidente grave – Incidente de segurança da informação de maior impacto para a organização, que prejudica de forma intensa a utilização dos serviços de TI ou expõe dados de forma indevida, devendo ser priorizado em relação aos demais incidentes.

4.1.8. Objetivo de Tempo de Recuperação (OTR/RTO) – Período de tempo gasto pela organização para recuperar uma atividade ou processo crítico após sua interrupção, que será definido em portaria específica.

4.1.9. Resposta a incidentes: Ação tomada para proteger e restaurar as condições operacionais dos sistemas de informação e as informações neles armazenadas, quando ocorre um ataque ou intrusão.

4.2. Esta norma visa descrever as principais estratégias no tratamento de incidentes computacionais, que envolvam ou não dados pessoais, permitindo a adequada preparação, detecção, contenção, erradicação, recuperação, avaliação e comunicação destes incidentes.

5. Da preparação

5.1. Deve ser criado um plano de resposta a incidentes, incluindo:

5.1.1. A definição de papéis e responsabilidades

5.1.2. A identificação dos ativos críticos

5.1.3. Principais tipos de incidentes e ameaças

5.1.4. A definição dos processos e procedimentos a serem seguidos durante o incidente.

5.2. Devem ser implementadas, no mínimo, as seguintes medidas preventivas:

5.2.1. Monitoramento de eventos de segurança;

5.2.2. Registro de log de eventos de segurança, de acordo com norma específica;

5.2.3. Cópias de segurança regulares, de acordo com norma específica;

5.2.4. Testes de segurança periódicos;

5.2.5. Treinamento de conscientização em segurança para os usuários.

5.3. Devem ser consultadas fontes públicas confiáveis e atualizadas com informações e alertas sobre ameaças cibernéticas, incidentes de segurança da informação e melhores práticas de segurança.

6. Da detecção e análise

6.1. Deve ser mantido um monitoramento contínuo da infraestrutura de modo que os incidentes de segurança sejam detectados logo que ocorram.

6.1.1. O monitoramento deve incluir, sempre que possível, sem prejuízo a outras ações:

6.1.1.1. Verificação rotineira dos eventos de segurança;

6.1.1.2. Uso de soluções de detecção de intrusões;

6.1.1.3. Análise de logs;

6.1.1.4. Acompanhamento dos alertas de segurança.

6.2. A detecção dos incidentes poderá ocorrer por meio de ferramentas automatizadas de monitoramento de eventos, pela análise manual de registros de eventos, por comunicação de usuários ou por monitoramento proativo das equipes técnicas.

6.3. Identificado um incidente de segurança ou a suspeita dele, devem ser seguidos os procedimentos previstos no Processo de Gerenciamento de Incidentes do Tribunal.

6.3.1. Confirmada a ocorrência de um incidente, o plano de respostas a incidentes pertinente deve ser iniciado.

6.4. Sempre que um incidente de segurança for detectado, deve ser feita uma análise inicial para entender sua natureza e a extensão.

6.5. A análise detalhada do incidente de segurança envolve determinar:

6.5.1. Como ele ocorreu;

6.5.2. Quais sistemas ou dados foram afetados;

6.5.3. Qual o impacto potencial.

6.6. As áreas técnicas envolvidas na resposta ao incidente devem, na medida do possível, atuar para preservar as evidências forenses para eventual análise posterior, tais como:

6.6.1. efetuar cópia completa do sistema comprometido;

6.6.2. efetuar cópia dos logs de acesso;

6.6.3. efetuar cópia de mensagens ou arquivos;

6.6.4. outras ações previstas no plano de resposta a incidentes respectivo.

7. Da contenção, erradicação e recuperação.

7.1. Devem ser adotadas todas as medidas necessárias para conter o incidente e evitar que ele se espalhe ou cause mais danos. Tais medidas podem envolver, dentre outras:

7.1.1. Suspensão do acesso a sistemas comprometidos;

7.1.2. Isolamento de redes afetadas;

7.1.3. Desativação temporária de serviços comprometidos.

7.2. Devem ser adotadas todas as medidas para erradicação completa do incidente, incluindo, dentre outras:

7.2.1. Localização da causa raiz.

7.2.2. Remoção de malwares ou afins;

7.2.3. Restauração de sistemas a um estado seguro;

7.2.4. Correção de falhas de segurança.

7.3. O processo de recuperação deve envolver a restauração completa dos sistemas, aplicativos ou dados afetados por meio de backups ou outras fontes confiáveis.

7.4. A recuperação do ambiente deve ocorrer somente após a certeza de que a ameaça e vulnerabilidade que deram causa ao incidente (causa raiz) foram adequadamente tratadas.

7.5. Em caso de incidente grave, a recuperação do ambiente deve ocorrer somente com aval do Gestor de Crises, ou por outra autoridade determinada pela presidência do TRE-ES.

8. Da avaliação pós-incidente

8.1. A avaliação pós-incidente consiste em analisar a eficácia da resposta e identificar as áreas de melhoria. Os procedimentos incluem:

8.1.1. Revisão de procedimentos e controles;

8.1.2. Identificação de lacunas na segurança da informação;

8.1.3. Executar medidas técnicas para evitar futuros incidentes semelhantes.

8.1.4. Adoção de ações disciplinares ou legais, dependendo da natureza e da gravidade do incidente.

8.2. Os procedimentos realizados e as lições aprendidas devem ser documentados em um relatório de incidente.

8.2.1. O relatório de incidente deverá ser armazenado em sistema de informação específico e ter o seu acesso restrito a quem for de direito.

8.3. Se por algum motivo a causa raiz não possa ser adequadamente determinada, a ETIR deverá registrar como problema para análise posterior.

9. Da comunicação

9.1. Todas as partes interessadas devem ser comunicadas no caso de um incidente de segurança, incluindo: equipe técnica, gestores, usuários afetados e, quando for o caso, autoridades reguladoras ou órgãos responsáveis pela aplicação da lei.

9.1.1. Nos casos em que o incidente de segurança cibernética envolva destruição, perda, alteração, divulgação ou acessos não autorizados, de forma acidental ou ilícita, a dados pessoais transmitidos, armazenados ou processados pelo Tribunal o encarregado de dados deverá ser comunicado.

9.2. A comunicação deve fornecer informações precisas e claras sobre o tipo do incidente, suas consequências e as medidas adotadas pela contenção e recuperação.

9.3. Deve ser estabelecido um plano de comunicação de crise para garantir que as informações sejam transmitidas de maneira apropriada e coordenada.

9.4. Em caso de incidentes graves envolvendo dados pessoais, o Encarregado de Dados Pessoais informará à ANPD e aos titulares dos dados, de acordo com o plano de comunicação.

9.5. A comunicação externa com a sociedade em caso de incidentes graves cabe ao Comitê de Crises Cibernéticas.

10. Das responsabilidades

10.1. À Equipe de respostas a incidentes de Segurança Cibernética (ETIR) cabe:

10.1.1. Elaborar o plano de resposta a incidentes e acioná-lo em caso de ocorrência de um incidente de segurança;

10.1.2. Estabelecer os meios de comunicação oficiais e adicionais a serem acionados durante o processo de resposta à incidentes;

10.1.3. Conduzir o processo de análise, contenção, erradicação, recuperação dos incidentes de segurança.

10.1.4. Documentar os procedimentos realizados e as lições aprendidas, por meio de relatório de incidente.

10.2. À área técnica responsável pelos ativos de rede:

10.2.1. Manter o registro de *logs* de eventos de segurança, de acordo com norma específica, com intuito de subsidiar a detecção manual ou automatizada de incidentes.

10.2.2. Efetuar o monitoramento contínuo da infraestrutura de rede.

10.2.3. 10.2.3. No âmbito do Tribunal, a área técnica responsável pelos ativos de rede é a Seção de Gestão de Infraestrutura e Redes no TRE-ES.

10.3. À área técnica responsável pela segurança cibernética:

10.3.1. Monitorar as ameaças cibernéticas na infraestrutura de rede local e em nuvem com apoio das áreas técnicas responsáveis pelos ativos;

10.3.2. Acompanhar regularmente os boletins do CTIR.GOV, que contém informações e alertas sobre ameaças cibernéticas, zelando para que sejam adotadas as ações pertinentes.

10.3.3. Apoiar a ETIR no tratamento dos incidentes de segurança.

10.3.4. No âmbito do Tribunal, a área técnica responsável pela segurança cibernética é o Núcleo de Segurança Cibernética.

10.4. Ao Comitê de Crises Cibernéticas cabe:

10.4.1. A comunicação externa com a sociedade, em caso de incidentes graves, que inviabilizem as atividades precípuas do TRE-ES.

10.5. Ao Encarregado de dados cabe:

10.5.1. A comunicação com a ANDP e com os titulares de dados, em caso de incidentes graves envolvendo dados pessoais.

10.6. À Comissão de Segurança da Informação cabe:

10.6.1. O monitoramento das atividades da ETIR e o estabelecimento de métricas de desempenho.

10.7. Aos usuários cabe:

10.7.1. A comunicação imediata caso tenham a informação da ocorrência de quaisquer incidentes de segurança da informação, utilizando a CESTIC.

11. Das disposições finais

11.1. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação ou pelo Comitê Gestor de Proteção de Dados Pessoais, de acordo com o tipo do incidente.

11.2. O descumprimento não fundamentado desta norma deve ser comunicado à CSI, com consequente adoção das providências cabíveis.

11.3. Esta norma entra em vigor na data de sua publicação.

ANEXOS

ANEXO I - Plano de Gestão de Incidentes de Segurança

CONTROLE DE VERSÃO

Data	Versão	Descrição	Elaboração
06/02/2024	1.0	Versão inicial	NSC/CIS/STI

1. Introdução

O Plano de Gestão de Incidentes de Segurança é um conjunto de diretrizes, procedimentos e protocolos documentados do TRE-ES para responder eficazmente aos incidentes de segurança da informação. Seus principais objetivos são:

- Estabelecer ações para a detecção, resposta e tratamento dos incidentes de segurança;
- Garantir a coleta e preservação de evidências para apuração do incidente e encaminhamento às autoridades competentes;
- Restaurar a rede e os sistemas à normalidade o mais rápido possível; e
- Garantir a conformidade com as regulamentações de segurança e privacidade de dados.

2. Conceitos

Antimalware: Ferramenta utilizada para detecção e tratamento de programas maliciosos.

ETIR: Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética.

Firewall: Dispositivo de uma rede de computadores, na forma de programa ou de equipamento físico, que tem por objetivo aplicar uma política de segurança àquela rede ou aplicativo.

Incidente de segurança da informação: Qualquer evento ou situação que comprometa a segurança, a integridade, a confidencialidade ou a disponibilidade de informações, sistemas, redes ou recursos de uma organização, podendo ser intencional (como ataques cibernéticos) ou não intencional (como erros humanos ou falhas de sistema).

Logs: Registros de eventos em equipamentos ou aplicações, que gravam informações sobre o evento, como: usuário, data e hora, descrição do que ocorreu e do local em que ocorreu.

MFA: Múltiplo fator de autenticação, por meio do qual, além do login e da senha, exige-se do usuário pelo menos mais uma confirmação, como o uso de um token, um código em um autenticador, uma verificação por e-mail, biometria, entre outras.

3. Fases do Plano de Gestão de Incidentes de Segurança

O Plano de Gestão de Incidentes de Segurança é composto pelas seguintes fases:

- Preparação
- Detecção
- Contenção
- Erradicação
- Recuperação

3.1. Preparação

A preparação para tratar de um incidente de segurança consiste em:

- Publicação e divulgação das políticas de segurança da informação vigentes no Tribunal;
- Manutenção de registros de eventos de forma centralizada, em conformidade com a NSI 007 - Norma de gerenciamento de logs, para permitir a verificação na ocasião de um incidente de segurança;
- Realização de monitoramento constante do ambiente para permitir a detecção de um incidente; e
- Instituição e treinamento de uma Equipe de Tratamento de Incidentes de Segurança (ETIR) para tratar e responder a um incidente de segurança.
    - No TRE-ES, a gestão de incidentes cibernéticos é realizada pela Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR), estabelecida por meio do Ato 339/2022, em que foram definidos os membros da equipe, suas atribuições, responsabilidades e forma de atuação.

3.2. Detecção

Incidentes de segurança representam uma ameaça à segurança da informação e podem ter sérias consequências.

A detecção de um incidente de segurança pode ocorrer de várias formas:

- um usuário pode reportar um incidente;
- o monitoramento das ferramentas de segurança pode indicar um comportamento anômalo, que pode ser resultado de um incidente; ou
- uma ferramenta de segurança pode disparar um relatório reportando um incidente.

Dependendo da gravidade do incidente de segurança, será necessário realizar comunicações internas e externas sobre o ocorrido. A comunicação interna deverá seguir o estabelecido na Portaria 236/2022 do TRE-ES, que institui o comitê de crises cibernéticas e define a sala de situação. Externamente, os incidentes graves que ocasionam a deflagração de uma crise cibernética deverão ser comunicados ao Tribunal Superior Eleitoral e ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), órgão superior vinculado ao CNJ.

3.3. Contenção de Incidentes de Segurança

Alguns incidentes de segurança podem acarretar a lentidão ou a indisponibilidade de servidores, da rede corporativa, de dados ou de serviços, e até levar à exposição ou sequestro de dados. Nesses casos, é necessário realizar a contenção do incidente de segurança, ou seja, isolar o ambiente afetado de forma a impedir que o incidente se espalhe ou que continue seus efeitos sobre a rede ou demais sistemas e serviços.

O isolamento do incidente consiste em separar da rede o ambiente afetado ; desligar os equipamentos afetados e desativar as contas de usuários envolvidas.

Essa contenção permite a cópia dos dados para a realização da coleta de evidências, que inicia com uma documentação preliminar, que consiste no registro de informações iniciais sobre o incidente, como data, hora, descrição do incidente, além das contas de usuários, serviços, equipamentos e sistemas envolvidos.

3.3.1. Identificação de Evidências:

As evidências do incidente podem ser obtidas por meio da análise de:

- Registros de Sistemas: Coleta de registros de logs de sistemas, incluindo logs de segurança, logs de erros e logs de acesso.

- Registros de Rede: Captura de registros de tráfego de rede, como logs de firewalls, roteadores e switches.
- Registros de Equipamentos Servidores: Coleta de registros dos equipamentos servidores envolvidos, como logs de servidores web, bancos de dados, aplicativos etc.
- Registros de Aplicativos: Coleta de registros específicos de aplicativos relevantes para o incidente, se houver.
- Capturas de Tráfego: Realização de capturas de pacotes para análise detalhada do tráfego de rede, se necessário.
- Imagens de Disco: Realização de cópia de discos rígidos ou servidores para preservação de evidências digitais.

3.3.2. Preservação de Evidências

Após coletadas, as evidências devem ser preservadas para envio às autoridades competentes visando à investigação do incidente. Deve-se seguir as seguintes recomendações para preservar as evidências:

- Evitar Alterações: Garantir que as evidências coletadas não sejam alteradas. Trabalhar em cópias dos dados sempre que possível.
- Armazenamento Seguro: Manter as evidências em locais seguros e controlados para evitar adulteração.
- Cadeia de Custódia: Manter uma cadeia de custódia para documentar quem teve acesso às evidências e quando.
- Registros Detalhados: Manter um registro detalhado de todas as ações tomadas durante a coleta de evidências.

3.3.3. Relatório Final

Elaborar um relatório final que inclua uma descrição detalhada do incidente, evidências coletadas e recomendações para mitigação e prevenção futura.

3.4. Erradicação

Nesta fase, são realizadas ações para eliminar as ameaças presentes no ambiente do TRE-ES. São utilizadas ferramentas antimalware para eliminar softwares maliciosos do ambiente; é realizado o bloqueio das contas de usuários utilizadas como vetores para o

incidente ou a alteração de senhas e adoção de MFA para autenticação desses usuários; é feita a verificação do caminho de ataque utilizado no incidente para bloquear endereços IPs, fechar portas desnecessárias, adicionar sítios às listas de bloqueio de acesso, e demais ações necessárias para permitir a restauração do ambiente à estabilidade.

3.5. Recuperação e Normalização

Nesta fase, acontece a restauração de máquinas, sistemas e serviços desativados na fase de contenção.

Deve ser estabelecida uma rotina de monitoramento dos ativos afetados pelo incidente de segurança, para garantir que não há mais indícios de que o ataque ainda esteja acontecendo ou possa voltar a acontecer, assim como evitar a possibilidade de novos incidentes. Atividades que devem ser realizadas:

- Monitorar o tráfego de rede em busca de atividades incomuns ou padrões suspeitos que possam indicar atividade maliciosa;
- Monitorar os registros de sistemas, aplicativos e servidores em busca de eventos de segurança relevantes;
- Verificar se o antivírus está atualizado e realizar verificações completas em todos os sistemas para garantir que não haja malware persistente;
- Identificar e corrigir vulnerabilidades em sistemas e aplicativos;
- Monitorar o acesso de usuários a sistemas e aplicativos para identificar atividades não autorizadas ou alterações em privilégios;
- Monitorar os logs de firewall para detectar tráfego suspeito ou tentativas de acesso não autorizado;
- Monitorar e avaliar a segurança de aplicativos e códigos para identificar vulnerabilidades e garantir que boas práticas de segurança sejam seguidas;
- Implementar programas de treinamento e conscientização em segurança cibernética para educar os funcionários e prevenir futuros incidentes; e
- Atualizar este plano incluindo novos procedimentos identificados na análise do incidente.

Ao final, deve ser elaborado um relatório detalhado contendo todas as informações referentes ao incidente, tais como uma análise detalhada do incidente; todas as ações tomadas para contenção e divulgação do incidente e recuperação do ambiente; todas as

ações de segurança implementadas para conter novas ocorrências do incidente; além das lições aprendidas e das recomendações para o futuro.

ANEXO II – MODELO DO RELATÓRIO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA CIBERNÉTICA

DADOS GERAIS:

Nº da Ocorrência/Ano:			
Nome do agente responsável pela preservação dos dados do incidente:			
Matrícula:		Telefone:	
Endereço eletrônico:			
Nome do responsável pela ETIR:			
Matrícula:		Telefone:	
Endereço eletrônico:			
Nome do Órgão/Instituição:			
Endereço:			

RELATO SOBRE O INCIDENTE:

DESCREVA O INCIDENTE:
SE POSSÍVEL, DESCREVA A ORIGEM DO INCIDENTE, OU A RAZÃO DE NÃO SER POSSÍVEL IDENTIFICÁ-LA:
COMO FOI DETECTADO O INCIDENTE?
QUAIS FORAM OS DADOS COLETADOS E PRESERVADOS?
OUTROS DADOS JULGADOS RELEVANTES:
QUAIS FORAM AS AÇÕES DE TRATAMENTO E RESPOSTA AO INCIDENTE?
COMO FORAM PRESERVADOS OS REGISTROS DO INCIDENTE? QUAIS AS FERRAMENTAS UTILIZADAS?

QUAL FOI O LOCAL DE ARMAZENAMENTO DAS INFORMAÇÕES PRESERVADAS?

Local e data:

_____
Assinatura do agente responsável pela preservação dos dados do incidente

ANEXO III - PLANO DE COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS

CONTROLE DE VERSÕES

Versão 1.0	Maio/2025	Versão inicial aprovada pela CSI em 13/05/2025

SUMÁRIO

1 Introdução

2 Objetivos

3 Termos e Definições

4 Atores e Responsabilidades

5 Incidentes de Segurança com Dados Pessoais

6 Detalhamento do Plano de Comunicação de Incidentes

7 Disposições Finais

8 Fluxo do Procedimento

9 Referências

1. **INTRODUÇÃO**

Escândalos de vazamentos de dados e de ataques cibernéticos tornaram-se comuns atualmente e são provenientes de meios cada vez mais sofisticados para burlarem os controles e as medidas de segurança da informação.

Considerando o volume de dados que o Tribunal Regional Eleitoral do Espírito Santo (TRE/ES) trata, e a relevância de seu papel institucional na entrega de serviços públicos, é importante que o órgão esteja consciente de que incidentes de segurança tornaram-se uma realidade possível, e devem ser evitados com medidas de salvaguarda e prevenção.

Conforme definição constante no art. 4º do GDPR - General Data Protection Regulation - Regulamento Geral de Proteção de Dados, e tendo em vista que o TRE/ES custodia dados pessoais dos seus eleitores, é imprescindível que esteja preparado para agir em caso de "violação da segurança que provoque, de modo acidental ou ilícito a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento".

A LGPD (Lei Geral de Proteção de Dados Pessoais) trata dos incidentes de segurança que envolvam dados pessoais de forma muito rígida e o TRE deve estar preparado para atender às suas exigências, caso se veja envolvido em uma situação de risco.

> *Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.*
> *§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:*
> *I - a descrição da natureza dos dados pessoais afetados;*
> *II - as informações sobre os titulares envolvidos;*
> *III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;*
> *IV - os riscos relacionados ao incidente;*
> *V - os motivos da demora, no caso de a comunicação não ter sido imediata; e*
> *VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.*
> *§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:*
> *I - ampla divulgação do fato em meios de comunicação; e*
> *II - medidas para reverter ou mitigar os efeitos do incidente.*
> *§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.*

A Política Geral de Privacidade e Proteção de Dados Pessoais da Justiça Eleitoral, instituída pela Resolução nº 23.650/2021, preconiza que as unidades administrativas da Justiça Eleitoral devem informar à Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) os incidentes de segurança que representem risco ou dano relevante aos titulares de dados pessoais, na forma e nos termos da Política de Segurança da Informação da Justiça Eleitoral (PSI-JE), da NSI-014 do TRE/ES e da LGPD. A ETIR deverá comunicar o fato ao Encarregado, caso verifique a presença de risco ou de dano aos titulares.

A comunicação da ocorrência de incidente de segurança à autoridade nacional e ao titular de dados deverá ser realizada pelo controlador, por meio do Encarregado de Dados.

As medidas a serem adotadas no caso de uma situação de emergência ou evento de risco que ocasione danos aos titulares de dados e à própria instituição devem ser de conhecimento de todos os magistrados, servidores, terceirizados e demais colaboradores do TRE-ES, de modo a viabilizar que a comunicação apropriada seja feita de forma tempestiva à ANPD e aos afetados, quando for o caso.

2. **OBJETIVOS**

Objetivo Geral:

Orientar os magistrados, servidores, terceirizados e demais colaboradores do TRE-ES, nas respostas aos incidentes de segurança da informação envolvendo dados pessoais.

Objetivos Específicos:

* Definir os procedimentos a serem adotados na ocorrência de incidente de segurança da informação envolvendo dados pessoais, com os respectivos responsáveis.
* Assegurar respostas rápidas, efetivas e coordenadas, para atender ao prazo legal.
* Garantir a comunicação adequada às partes interessadas.
* Preservar a integridade, a disponibilidade e a confidencialidade das informações.
*Resguardar as evidências que possam ajudar a prevenir novos incidentes e atender às exigências legais de comunicação e transparência.

3. **TERMOS E DEFINIÇÕES**

Para fins deste documento, aplicam-se as seguintes definições:

Agentes de tratamento: corresponde ao Controlador e ao Operador. Não são considerados controladores ou operadores os indivíduos subordinados, tais como os funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento;

Anonimização: é a utilização de meios técnicos razoáveis e disponíveis por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

Ataque: evento de exploração de vulnerabilidades. Ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;

Autoridade Nacional de Proteção de Dados (ANPD): é o órgão da administração pública nacional responsável por fiscalizar e zelar pelo cumprimento da Lei Geral de Proteção de Dados em todo o território brasileiro;

Controlador: é o Tribunal Regional Eleitoral, representado pelo Presidente, a quem competem decisões referentes ao tratamento de dados pessoais;

Dados pessoais: informação relacionada à pessoa natural identificada ou identificável;

Dados pessoais sensíveis: são dados pessoais que dizem respeito a 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;

Encarregado pelo Tratamento de Dados Pessoais (Encarregado de Dados) ou Data Protection Officer (DPO): pessoa indicada pelo controlador ou operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

Operador: toda pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador;

RIPD: Relatório de Impacto à Proteção de Dados Pessoais

Sistemas: hardware, software, network de dados, armazenador de mídias e demais sistemas usados, adquiridos, desenvolvidos, acessados, controlados, cedidos ou operados pelo TRE-ES para dar suporte na execução de suas atividades.

Tratamento: qualquer operação ou conjunto de operações efetuadas sobre os dados, por meios automatizados ou não, incluindo, mas não se limitando, a coleta, gravação, organização, estruturação, alteração, uso, acesso, divulgação, cópia, transferência, armazenamento, exclusão, combinação, restrição, adaptação, recuperação, consulta, destruição ou anonimização;

Vazamento de dados: qualquer quebra de sigilo ou vazamento de dados que possa resultar, criminosamente ou não, na perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados não autorizado;

4. ATORES E RESPONSABILIDADES

Dentre os principais responsáveis pelas medidas a serem tomadas, em caso de incidente de segurança envolvendo dados pessoais, estão:

Comitê de Crises Cibernéticas do Tribunal Regional Eleitoral do ES: comitê responsável por promover o gerenciamento adequado de crises, por meio de resposta rápida e eficiente a incidentes em que os ativos de informação do TRE/ES tenham a sua integridade, confidencialidade ou disponibilidade comprometidas por longo período, ou quando tenha grande impacto à imagem da instituição, nos termos da Portaria PRE n. 236, de 04 de julho de 2022.

Comitê Gestor de Proteção de Dados Pessoais (CGPD): comitê responsável, em última instância, pela implementação da LGPD no TRE-ES, e por decidir, com base nas informações do Encarregado de Dados, sobre a comunicação do incidente de segurança à ANPD e aos titulares de dados (instituído pelo Ato n. 82, de 11/03/2021, alterado pelo Ato n. 181, de 02 de maio de 2024).

Comissão de Segurança da Informação do TRE-ES (CSI): comitê responsável, dentre outras atribuições, por acompanhar os processos de segurança da informação e de proteção de dados pessoais, nos termos do Ato PRE n. 171, de 26/04/2024).

Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR): grupo de servidores com responsabilidade de receber, analisar e responder as notificações e atividades relacionadas a incidentes de segurança da informação. Quando se tratar de incidente de segurança que envolva dados pessoais, a ETIR comunicará o ocorrido ao Encarregado de Dados, para as providências previstas na LGPD e no portal da ANPD sobre comunicação de incidentes de segurança, nos termos do Ato PRE n. 339, de 23/09/2022.

5. INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

Conforme art. 46 da LGPD, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, e tais medidas de segurança deverão ser observadas desde a concepção do produto ou serviço até a sua execução.

Em caso de incidente que comprometa a segurança de dados pessoais de potenciais titulares, a ETIR deverá comunicar o evento ao encarregado, conforme previsto no art. 17, inciso X, do Ato PRE n. 339, de 23/09/2022, incluindo, minimamente, as seguintes informações, nos termos do Guia de Resposta a Incidentes de Segurança do Governo Federal:

- impacto do evento;
- natureza;
- categoria e quantidade de titulares de dados pessoais afetados;
- categoria e quantidade de dados afetados;
- consequências do incidente para os titulares de dados e para o TRE-ES;
- criticidade

O Encarregado de Dados do Tribunal, após comunicação da ETIR e com apoio das áreas afetadas e do Grupo de Trabalho Técnico de Adequação do TRE-ES à LGPD, deverá adotar os seguintes procedimentos:

5.1 COMUNICAR A OCORRÊNCIA DO INCIDENTE AO CGPD

O Encarregado de Dados, após ser comunicado pela ETIR do incidente, registrará em controle próprio o evento, e reportará imediatamente as informações recebidas ao CGPD, sugerindo o agendamento de reunião em caráter extraordinário, em até 24 horas da notificação do evento pela ETIR, se entender necessário.

5.2 PREENCHER O FORMULÁRIO DE COMUNICAÇÃO À ANPD

Considera-se como medida de boa prática a interação do Encarregado de Dados com as unidades envolvidas, de modo a dar início ao preenchimento do formulário de comunicação à ANPD (Peticionamento Eletrônico

ANPD — Autoridade Nacional de Proteção de Dados), com as informações disponíveis no momento, e guardá-lo para futuro envio à ANPD, se assim for deliberado pelo CGPD.

Na medida em que outras informações forem sendo levantadas, essas deverão ser adicionadas ao formulário, para complementar o registro, dentro do prazo legal.

5.3 REUNIR COM O CGPD

Caso o CGPD entenda oportuna a realização de reunião, poderá convocar o Encarregado de Dados e demais equipes envolvidas no levantamento das informações, a fim de deliberar quanto à necessidade de comunicação ao Comitê de Crises Cibernéticas do TRE-ES, à ANPD e ao(s) titular(es) de dados afetados, bem como quanto à estratégia de comunicação externa e interna a ser executada pela assessoria de comunicação do Tribunal, se for o caso.

A comunicação à ANPD de Incidente de Segurança que possa acarretar risco ou dano relevante aos titulares, nos termos da Resolução CD/ANPD 15/2024, deve considerar os interesses e direitos fundamentais dos titulares e, cumulativamente, envolver, pelo menos, um dos seguintes critérios:

a - dados pessoais sensíveis;

b - dados de crianças, de adolescentes ou de idosos;

c - dados financeiros;

d - dados de autenticação em sistemas;

e - dados protegidos por sigilo legal, judicial ou profissional; ou

f - dados em larga escala.

Considera-se incidente com dados em larga escala aquele que abranger número significativo de titulares, considerando, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica de localização dos titulares.

Para apoiar a análise do incidente de segurança, os envolvidos poderão utilizar os Manuais de Gestão de Riscos adotados pelo TRE-ES.

5.4 COMUNICAR O INCIDENTE AO COMITÊ DE CRISE CIBERNÉTICA

Caso o CGPD entenda tratar-se de incidente de alto risco, convocará o Comitê de Crises Cibernéticas do TRE-ES, nos termos da Portaria PRE n. 236, de 04 de julho de 2022 para, mediante o apoio da Assessoria de Comunicação Institucional (ASCI) e de outras unidades do Tribunal envolvidas no incidente, detalhar a estratégia de comunicação com a imprensa, público em geral e titulares de dados afetados.

Para fins deste Plano, considera-se de alto risco o tratamento de dados pessoais que atender cumulativamente a pelo menos um critério geral e um critério específico, dentre os a seguir indicados:

I. critérios gerais:
   a. tratamento de dados pessoais em larga escala; ou
   b. tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares.

II. critérios específicos:
   a. uso de tecnologias emergentes ou inovadoras;

b. vigilância ou controle de zonas acessíveis ao público;
c. decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular; ou
d. utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

O tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais será caracterizado, dentre outras situações, naquelas em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

Os questionamentos a seguir servirão como parâmetro para a coleta de informações, que deverá ser realizada pela ASCI, podendo ser aprofundados e ajustados em consonância com as particularidades do incidente.

a. Quais informações foram objeto do incidente?
b. O titular pode ser vítima de fraude em razão do incidente?
c. O incidente foi devidamente comunicado às autoridades?
d. O que o titular pode fazer em benefício da sua proteção?
e. Onde o titular pode obter mais informações sobre o incidente?
f. A descrição da natureza dos dados pessoais afetados;
g. As informações sobre os titulares envolvidos;
h. A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
i. Os riscos relacionados ao incidente;
j. Os motivos da morosidade, no caso de a comunicação não ter sido imediata;
k. E as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

5.5 COMUNICAR O INCIDENTE À ANPD E AO(S) TITULAR(ES) DE DADOS PESSOAIS

Caso o CGPD entenda pertinente a notificação do incidente de segurança à ANPD, o Encarregado concluirá o preenchimento do formulário disponível no sítio eletrônico da Agência https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

O Controlador, por meio do Encarregado de Dados Pessoais do TRE/ES, será responsável por comunicar à ANPD o incidente de segurança ocorrido, **no prazo de até 3 (três) dias úteis**, nos termos da Resolução CD/ANPD nº 15, de 24 de abril de 2024 que aprova o Regulamento de Comunicação de Incidente de Segurança. As informações fornecidas poderão ser complementadas, de maneira fundamentada, no prazo de vinte dias úteis, a contar da data da comunicação.

Igualmente, deverá comunicar o incidente, de forma direta e individual sempre que possível, aos titulares cujos dados tiverem sido violados. Se, pela natureza do incidente, não for possível identificar individualmente os titulares afetados, devem ser comunicados todos os presentes na base de dados comprometida.

A comunicação poderá se dar por quaisquer meios tais como SMS, e-mail, reuniões, mensagem eletrônica, ou por outro meio que seja mais adequado ao contexto.

A ANPD orienta que as informações prestadas aos titulares de dados devem ser claras e concisas. Recomenda ainda que a comunicação mencione, no que couber, os elementos previstos nos incisos do §1º do art. 48 da LGPD, tais como:

a. a descrição da natureza dos dados pessoais afetados;
b. as informações sobre os titulares envolvidos;
c. a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
d. os riscos relacionados ao incidente;
e. os motivos da demora, no caso de a comunicação não ter sido imediata; e
f. as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

À ANPD, deverão ser fornecidas as seguintes informações:

- A descrição da natureza e da categoria de dados pessoais afetados;
- O número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;
- As medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente, observados os segredos comercial e industrial;
- Os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;
- Os motivos da demora, no caso de a comunicação não ter sido realizada no prazo previsto no caput deste artigo;
- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;
- A data da ocorrência do incidente, quando possível determiná-la, e a de seu conhecimento pelo controlador;
- Os dados do encarregado ou de quem represente o controlador;
- A identificação do controlador e, se for o caso, declaração de que se trata de agente de tratamento de pequeno porte;
- A identificação do operador, quando aplicável;
- A descrição do incidente, incluindo a causa principal, caso seja possível identificá-la; e
- O total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.

Quando houver indícios de crime, de acordo com a Lei nº 12.737, de 30 de novembro de 2012, ou outras normas presentes na legislação penal extravagante, o Controlador deverá comunicar à Polícia Federal, por meio de instrumento que entender mais adequado.

5.6 ELABORAR RELATÓRIO FINAL

A elaboração do Relatório Final é de responsabilidade do Encarregado de Dados. Se necessário, poderá solicitar o apoio da ETIR, da Comissão de Segurança da Informação do Tribunal, do Comitê Gestor de Proteção de Dados Pessoais (CGPD) e das áreas envolvidas no incidente.

O relatório deve conter o máximo de informações e evidências que tiverem sido coletadas durante a investigação do incidente, bem como o registro das deliberações das equipes envolvidas. Além disso, deve:

a) discriminar as ações realizadas pelas equipes envolvidas, para o tratamento efetivo do incidente e mitigação dos seus efeitos;
b) conter considerações sobre a promoção da melhoria contínua dos processos de tratamento de incidentes;
c) estar disponível para consulta em caso de atualização do Relatório de Impacto à Proteção de Dados (RIPD);
d) ser devidamente armazenado, para atender eventual demanda de órgãos fiscalizadores, em consonância com o princípio da responsabilização e prestação de contas (art. 6º, X da LGPD).

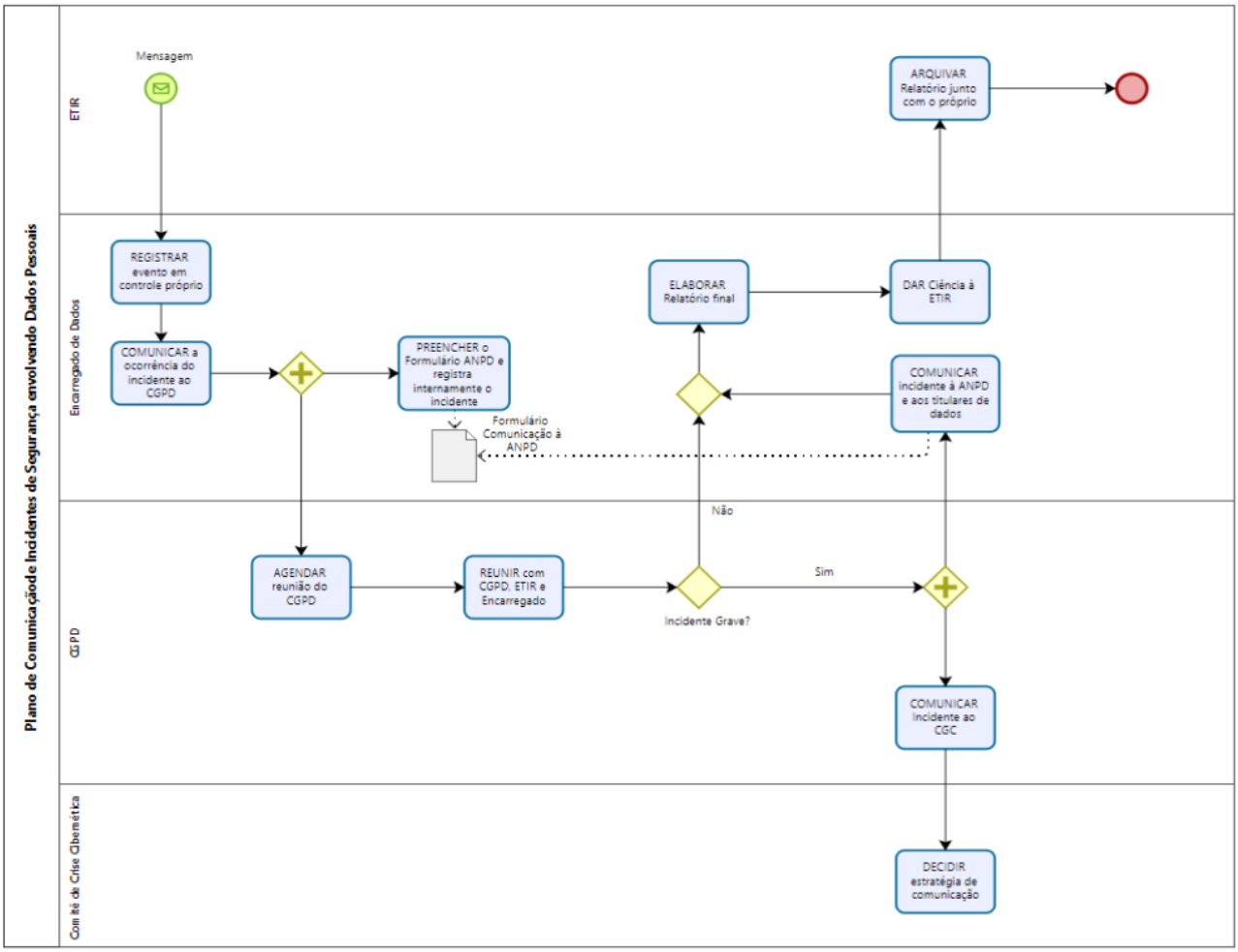
5.7 DAR CIÊNCIA À ETIR DO TRE-ES

Após as medidas de tratamento empreendidas e o registro das ações em processo administrativo eletrônico restrito, o Encarregado de Dados encaminhará o relatório final à ETIR, comunicando o desfecho do incidente de segurança envolvendo dados pessoais.

6. DISPOSIÇÕES FINAIS

Caso a ANPD, no exercício de suas competências legais, preveja procedimentos e prazos diversos dos estabelecidos neste Plano, prevalecerão aqueles definidos pela Autoridade.

7. PROCESSO DE COMUNICAÇÃO



8. REFERÊNCIAS

Lei nº 13.709/2021 - Lei Geral de Proteção de Dados Pessoais (LGPD)
Resolução TSE nº 23.650/2021 - Institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral.
Resolução nº 2/2022, da ANPD – Indica critérios para definição de Alto Risco.
Resolução nº 15/2024, da ANPD - Regulamento de Comunicação de Incidente de Segurança.
Resolução nº 18/2024, da ANPD - Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais.
Portaria PRE/TRE-ES nº 236/2022 - Institui o Comitê de Crises Cibernéticas no Tribunal Regional Eleitoral do Espírito Santo e define a Sala de Situação.
Ato nº 181/2024 - Atual composição do Comitê Gestor de Proteção de Dados Pessoais (CGPD) do TRE-ES
Ato PRE n. 171/2024 - Designa o Gestor de Segurança da Informação do TRE/ES
Ato PRE nº 339/2022 - Dispõe sobre a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) no âmbito do TRE-ES
Guia de Resposta a Incidentes de Segurança do Governo Federal
NSI-014 - Gestão de Incidentes de Segurança da Informação - Estabelece as principais estratégias no tratamento de incidentes computacionais, que envolvam ou não dados pessoais, permitindo a adequada preparação, detecção, contenção, erradicação, recuperação, avaliação e comunicação destes incidentes.

Manual de Gestão de Riscos do TRE-ES

ANEXO IV - RELATÓRIO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS
(Processo nº .../2025)

1. Apresentação

Breve descrição da organização (TRE-ES), do sistema/serviço afetado e do incidente.
Orientação: Indicar, de forma objetiva, onde ocorreu o incidente, qual sistema, serviço ou processo foi afetado e qual a natureza do evento (ex.: vazamento de dados, ataque de ransomware, indisponibilidade de sistema, acesso não autorizado).

2. Resumo Executivo

Síntese das informações coletadas e das ações realizadas.
Orientação: Informar data e hora de ocorrência/detecção, sistemas impactados, equipe responsável pela coordenação da resposta, medidas tomadas (ex.: isolamento de máquinas, bloqueio de acessos, comunicação interna), resultados iniciais e estado atual.

3. Análise do Incidente

Descrição detalhada do ocorrido.
Orientação: Incluir informações técnicas (logs, registros de auditoria, evidências coletadas), causas identificadas (falha humana, vulnerabilidade técnica, ataque externo, negligência), e análise preliminar de impactos.

4. Nível de Prioridade, Escalonamento e Elevação

Classificação do incidente quanto à gravidade e impacto.
Orientação: Utilizar critérios Crítico / Alto / Médio / Baixo. Documentar se houve necessidade de escalonamento (reforço de equipe técnica) ou elevação (envolvimento da alta gestão ou comunicação imediata ao TSE/ANPD).

5. Avaliação de Risco e Dever de Comunicação

Resultado da análise de risco e decisão quanto à comunicação aos titulares e à ANPD.
Orientação: Avaliar se o incidente pode gerar risco ou dano relevante aos titulares (fraude, discriminação, exposição de dados sensíveis, riscos reputacionais). Se sim, registrar decisão e plano de comunicação:
a) Titulares – forma e prazo de comunicação.
b) ANPD – observância da Resolução CD/ANPD nº 15/2024.
c) Outros órgãos de controle – quando aplicável (ex.: CNJ, TSE).

6. Ações Imediatas e Medidas de Contenção

Registro das providências técnicas e administrativas adotadas.
Orientação: Indicar isolamento de sistemas, aplicação de patches, troca de senhas, comunicação ao time de resposta a incidentes, abertura de chamados, acionamento de fornecedores ou terceiros, quando houver.

7. Medidas de Recuperação

Ações para retorno à normalidade.

Orientação: Indicar prazos de restauração de sistemas, recuperação de backups, restabelecimento de serviços e monitoramento pós-incidente.

8. Recomendações e Medidas Preventivas

Orientação: Listar vulnerabilidades corrigidas, planos de melhoria, reforço em controles de acesso, implementação de políticas internas, ações de conscientização de usuários, e elaboração/revisão de Relatório de Impacto à Proteção de Dados (RIPD), quando aplicável.

9. Conclusão

Síntese final, destacando os principais aprendizados, medidas adotadas e necessidade de ações de médio/longo prazo.

Orientação: Indicar se o incidente foi totalmente resolvido, se há monitoramento em curso e quais medidas estruturantes serão incorporadas ao Programa de Privacidade e Segurança da Informação do TRE-ES.

Vitória/ES, [data]

[Nome do Encarregado]
Encarregado pelo Tratamento de Dados Pessoais – TRE-ES