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.