

DIRETORIA GERAL

INSTRUÇÃO NORMATIVA DG Nº 3, DE 20 DE MARÇO DE 2023.

INSTRUÇÃO NORMATIVA DG Nº 3, DE 20 DE MARÇO DE 2023.

Dispõe sobre as regras e os procedimentos para gestão de incidentes de segurança da informação do Tribunal Regional Eleitoral do Rio de Janeiro.

A DIRETORA-GERAL DO TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO, no uso das atribuições que lhe são conferidas pelo art. 9º, I, da Resolução TRE nº 1.107, de 30 de setembro de 2019 (Regulamento Administrativo do Tribunal Regional Eleitoral do Rio de Janeiro),

CONSIDERANDO a Resolução CNJ nº 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Resolução TSE nº 23.644, de 1º de julho de 2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO as boas práticas em segurança da informação previstas nas normas ABNT ISO /IEC 27001 e ABNT NBR ISO/IEC 27002;

CONSIDERANDO as boas práticas de resposta a incidentes previstas no guia NIST SP-800-61rev. 2;

CONSIDERANDO a necessidade de gerenciar os incidentes de segurança da informação que envolvam dados pessoais, de acordo com a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD);

CONSIDERANDO que a segurança da informação e a proteção de dados pessoais são condições essenciais para a prestação dos serviços jurisdicionais e administrativos do Tribunal Regional Eleitoral do Rio de Janeiro; e

CONSIDERANDO, ainda, o disposto no processo SEI nº 2022.0.000054244-0,

RESOLVE:

CAPÍTULO I DAS DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a norma de gestão de incidentes de Segurança da Informação no âmbito do TRE-RJ.

Art. 2º Esta norma integra a Política de Segurança da Informação da Justiça Eleitoral, estabelecida pela Resolução TSE nº 23.644/2021.

Art. 3º O presente normativo tem por objetivo descrever as principais estratégias no tratamento e resposta a incidentes de Segurança da Informação que envolvam ou não dados pessoais, permitindo a adequada preparação, detecção, análise, contenção, erradicação, recuperação, avaliação e comunicação desses incidentes.

Art. 4º O ciclo de gestão de incidentes de segurança da informação no TRE-RJ é

composto das seguintes etapas:

- I. - preparação;
- II. - detecção e análise;
- III. - contenção, erradicação e recuperação;
- IV. - atividades pós-incidente.

Art. 5º A gestão de incidentes em segurança da informação deve observar o Protocolo de Prevenção de Incidentes Cibernéticos no âmbito do Poder Judiciário (PPINC-PJ), o Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Poder Judiciário (PGCRC-PJ) e o Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário (PIILC-PJ), todos integrantes da Política de Segurança Cibernética do Poder Judiciário (PSEC-PJ), instituída pelo Conselho Nacional de Justiça (CNJ).

CAPÍTULO II

DAS DEFINIÇÕES

Art. 6º Para efeitos desta norma consideram-se os seguintes termos e definições, aplicando-se subsidiariamente os previstos na Portaria DG nº 444, de 8 de julho de 2021, do Tribunal Superior Eleitoral:

- I. - ANPD: Agência Nacional de Proteção de Dados Pessoais;
- II. - CTIR GOV: Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo;
- III. - ETIR (Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética): Equipe de tecnologia da informação, de constituição multidisciplinar, coordenada por um agente responsável;
- IV. - 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.;
- V. - Incidente de Segurança da Informação: Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de informação ou das redes de computadores;
- VI. - Incidente de Segurança da Informação com dados pessoais: Qualquer incidente de segurança à proteção de dados pessoais, como acesso não autorizado e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento de dados ilícita ou inadequada;
- VII. - 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;
- VIII. - 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.

CAPÍTULO III

DAS RESPONSABILIDADES

- Art. 7º A atuação operacional na resposta a incidentes é de responsabilidade da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética - ETIR - e suas atribuições e modo de funcionamento estão previstas em sua norma constitutiva e regulamentar.
- Art. 8º Cabe a todos os usuários internos a comunicação imediata caso tenham a informação da ocorrência de quaisquer incidentes de segurança da informação, utilizando os canais próprios fornecidos pela STI.

CAPÍTULO IV

DA PREPARAÇÃO

- Art. 9º A ETIR elaborará o seu processo de trabalho e planos de resposta específicos a incidentes (playbooks), contendo os passos do processo de resposta, de acordo com os principais tipos de incidentes e ameaças, os quais ficarão disponíveis para consulta dos seus componentes.
- Art. 10. A ETIR determinará os meios de comunicação oficiais e adicionais a serem acionados durante o processo de resposta a incidentes.
- Art. 11. A ETIR manterá lista atualizada com os contatos de todos os integrantes da sua equipe.
- Art. 12. O Núcleo de Defesa Cibernética - NDEC - fará o monitoramento de ameaças cibernéticas, incluindo o acompanhamento de boletins encaminhados pelo CTIR GOV.

CAPÍTULO V

DA DETECÇÃO E ANÁLISE

- Art. 13. 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 dos operadores técnicos.
- Art. 14. Detectado o incidente ou a suspeita dele a ETIR procederá ao registro e à análise necessária, abrangendo:
- I. - o resumo do incidente;
 - II. - a categoria do incidente;
 - III. - a identificação dos recursos afetados e a avaliação do impacto nestes e em outros recursos;
 - IV. - a estimativa da criticidade e urgência;
 - V. - a priorização do tratamento do incidente, levando em conta a severidade de seu impacto nonegócio e a urgência de sua resolução.

Parágrafo único. A categorização e a priorização do tratamento de incidentes observarão o disposto no Anexo desta norma.

Art. 15. Confirmada a ocorrência do incidente, a ETIR acionará o plano de resposta adequado e comunicará à Assessoria de Segurança da Informação e, se for o caso, ao Encarregado de Dados Pessoais.

Art. 16. As áreas técnicas envolvidas na resposta ao incidente, na medida do possível, atuarão para preservar evidências forenses para eventual análise, devendo:

- I. - efetuar cópia completa do sistema comprometido;
- II. - efetuar cópias dos logs de acesso;
- III. - efetuar cópias de mensagens ou arquivos;
- IV. - outras ações previstas no plano de resposta a incidentes respectivo e no Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ).

Parágrafo único. A ETIR deverá fazer constar em relatório a eventual impossibilidade de preservação das mídias afetadas e listar os procedimentos adotados.

Art. 17. Quando o incidente de segurança caracterizar-se como uma crise cibernética, o Comitê de Crises Cibernéticas deverá ser acionado, nos termos do Protocolo de Gerenciamento de Crises Cibernéticas (Ato GP n.º 185/2022), sem prejuízo de outras ações que possam ser identificadas pelo Comitê de Crises Cibernéticas e/ou pela ETIR.

CAPÍTULO VI

DA CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO

Art. 18. Após a fase de detecção e análise, a ETIR atuará para conter os danos causados pelo incidente, localizar a causa raiz e erradicar a ameaça, além de promover a recuperação dos ativos, respeitando seu nível de autonomia e as deliberações dos níveis superiores de gestão.

Art. 19. Durante a fase de contenção, erradicação e recuperação a ETIR deverá:

- I. - conter o incidente e, se possível, adotar soluções de contorno para manter a funcionalidade dos sistemas;
- II. - propor, validar e testar solução definitiva, em conjunto com as áreas envolvidas;
- III. - erradicar o incidente;
- IV. - remover códigos maliciosos;
- V. - identificar e tratar todas as vulnerabilidades que foram exploradas;
- VI. - retornar os sistemas afetados ao estado normal de operação.

§ 1º A recuperação do ambiente deve ocorrer somente após a certeza de que a ameaça e a vulnerabilidade que deram causa ao incidente (causa raiz) foram adequadamente tratadas.

§ 2º As atividades de contenção, erradicação e recuperação devem ser devidamente registradas.

CAPÍTULO VII

DAS ATIVIDADES PÓS-INCIDENTE

- Art. 20. Concluídas as etapas de tratamento do incidente, a ETIR deverá documentar os procedimentos realizados e as lições aprendidas, por meio da elaboração de relatório do incidente. Art. 21. O armazenamento dos relatórios de incidentes deverá ocorrer em sistema de informação específico, tendo seu acesso restrito.
- Art. 22. Na hipótese de a causa raiz não poder ser adequadamente determinada, a ETIR deverá registrar como problema para análise posterior.

CAPÍTULO VIII

DAS COMUNICAÇÕES

- Art. 23. Em caso de incidente que possa acarretar risco ou dano relevante para titulares de dados pessoais controlados pelo TRE-RJ, o Presidente do Tribunal determinará ao Encarregado de Dados Pessoais que realize a comunicação à ANDP e aos titulares de dados.
- Parágrafo único. Cabe à Coordenadoria de Comunicação Social - COSOC - elaborar, juntamente com o Encarregado, o teor do comunicado aos titulares de dados afetados pelo incidente.
- Art. 24. Diante de incidente que envolva dados pessoais operados pelo Tribunal ou dados tratados em controladoria conjunta, o Presidente do TRE-RJ determinará a imediata comunicação às entidades controladoras dos dados.
- Art. 25. A comunicação externa com a sociedade, em caso de incidentes graves previstos no Protocolo de Gerenciamento de Crises, será realizada pelo Coordenador do Comitê de Crise Cibernéticas ou por outra autoridade determinada pelo Presidente do TRE-RJ.
- Art. 26. A ETIR encaminhará ao Assessor de Segurança da Informação e ao Encarregado de Dados Pessoais relatório resumido de todos os incidentes que envolvam dados pessoais, tão logo a violação de dados seja confirmada.
- Art. 27. A Assessoria de Segurança da Informação apresentará ao Comitê Gestor de Segurança da Informação - CGSI - e à ETIR do TSE as informações relevantes acerca dos incidentes graves ocorridos.
- Art. 28. A Presidência do Tribunal reportará ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário - CPTRIC-PJ - e ao Tribunal Superior Eleitoral os incidentes graves de segurança cibernética detectados.

CAPÍTULO IX

DAS DISPOSIÇÕES FINAIS

- Art. 29. Os casos omissos serão resolvidos pelo Diretor-Geral, ouvido, quando necessário, a Comissão de Segurança da Informação ou o Comitê Gestor de Proteção de Dados Pessoais, de acordo com a categoria do incidente.
- Art. 30. O descumprimento não fundamentado desta norma deve ser comunicado e registrado pelo Assessor de Segurança da Informação, com consequente adoção das providências cabíveis.
- Art. 31. Esta norma deve ser revisada a cada 3 (três) anos, ou antes, se necessário, pela

ETIR e encaminhada para nova apreciação do Assessor de Segurança da Informação e da Comissão de Segurança da Informação.

Art. 32. Esta Instrução Normativa entra em vigor na data de sua publicação.

ELINE IRIS RABELLO GARCIA DA SILVA

Diretor(a)- Geral Anexo Único

*Republicada pela ausência do anexo na publicação de 21/03/2023

ANEXO ÚNICO

TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO Diretoria-Geral

Anexo da IN DG nº 03/2023 - Norma de Gestão de Incidentes de Segurança da Informação

Tabela 1— CATEGORIAS DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO		
Categoria	Tipo	Descrição / Exemplos
Código malicioso	Vírus	Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. Podem ser propagados por e-mail, scripts, macro ou telefone celular
	Worm	Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador
	Bot ou botnet	Programa semelhante ao worm, mas que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente
	Rootkit	Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido
	Trojan (Cavalo de Troia)	Programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário
	Spyware	Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros
Coleta de Informações	Scanning (Varredura)	Ataques que enviam pedidos a um sistema para descobrir pontos fracos ou vulnerabilidades e executam testes para recolher informações sobre hosts, serviços e contas. Exemplos: fingerd, consultas DNS, ICMP, SMTP, etc.
	Sniffing	Observação e registro do tráfego de rede (escutas)
	Engenharia social	Coleta de informações a partir do ser humano com ou sem o uso da tecnologia (por exemplo, mentiras, truques, subornos ou ameaças)
Intrusão	Exploração de vulnerabilidades	Uma tentativa de comprometer um sistema ou interromper qualquer serviço, explorando vulnerabilidades do sistema (por exemplo, buffer overflow, backdoors, cross side scripts, etc.).
	Tentativas de login	Várias tentativas de login (cracking de senhas, força bruta)
	Ataque com assinatura desconhecida	Tentativa usando um exploit desconhecido
	Conta privilegiada comprometida	Comprometimento do funcionamento normal de um sistema ou aplicação (serviço). Pode ser causado remotamente por uma vulnerabilidade conhecida ou nova, mas também por acesso local não autorizado
	Conta não privilegiada comprometida	
	Aplicação comprometida	
Disponibilidade	DoS (Denial of Service)	Tipo de ataque no qual um sistema é bombardeado com tantos pacotes que ficam lentos e em alguns casos podem até travar. Exemplos de um DoS remoto são Syn flood, ping flood, etc. No entanto, a disponibilidade pode ser afetada também por ações locais (destruição, rompimento de fornecimento de energia, etc.).
	DDoS (Distributed DoS)	
	Sabotagem	
Segurança da Informação	Acesso não autorizado	A segurança da informação pode ser ameaçada por uma conta de usuário válida ou aplicação comprometida que permitam acesso não autorizado à informação. Há, ainda, ataques que interceptam e acessam informações durante a transmissão dos dados pela rede.
	Modificação não autorizada	
Fraude	Uso não autorizado dos recursos	Uso de recursos para fins não autorizados, incluindo ventures com fins lucrativos (por exemplo, o uso de e-mail para participar na cadeia de lucro ilegal ou esquemas de pirâmide)
	Direitos autorais (copyright)	Vender ou instalar cópias de software ou outros materiais protegidos por direitos autorais sem a devida licença

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO		
Categoria	Tipo	Descrição / Exemplos
	Masquerade	Tipos de ataques em que uma entidade ilegítima assume a identidade do outro, a fim de obter benefícios
Outros		Todos os incidentes não categorizados em um dos tipos anteriores devem ser classificados nesta classe. Quando o número de incidentes nesta categoria aumentar, será o momento de rever esta tabela de classificações.

(fonte: TRE-SP)

TABELAS 2, 3 E 4 - PRIORIZAÇÃO DE INCIDENTES

Para que seja estabelecida a priorização dos incidentes de Segurança da Informação devem ser considerados:

a) O Impacto no Negócio

A ETIR deve levar em conta o impacto negativo que o incidente pode causar nos negócios do Tribunal, incluindo os impactos futuros que podem atingir o órgão. A tabela abaixo traz os níveis de impacto no negócio.

Tabela 2

Categoria	Definição
Nenhum	Não afeta a capacidade da organização de fornecer todos os serviços a todos os usuários.
Baixo	Efeito mínimo; a organização ainda pode fornecer todos os serviços essenciais para todos os usuários, mas perdeu eficiência.
Médio	A organização perdeu a capacidade de fornecer um serviço crítico a um subconjunto de usuários do sistema.
Alto	A organização não é mais capaz de fornecer alguns serviços essenciais a nenhum usuário.

(fonte: Secretaria de Governo Digital do Ministério da Economia)

b) O Impacto em Dados e Informações

Deve ser avaliado o impacto do incidente na confidencialidade, integridade e disponibilidade dos dados e informações e sua repercussão na esfera do Tribunal, de entes parceiros e titulares de dados.

As categorias de impacto aos dados e informações estão previstas na seguinte tabela.

Tabela 3

Categoria	Definição
Nenhum	Nenhuma informação relevante foi exposta, alterada, excluída ou de alguma maneira comprometida.
Violação de privacidade	Informações confidenciais de identificação pessoal (DP) de contribuintes, funcionários, beneficiários etc. foram acessadas ou expostas.
Violação Proprietária	Informações proprietárias não classificadas, como informações de infraestrutura crítica protegida (PCII), foram acessadas ou expostas.
Perda de Integridade	Informações confidenciais ou proprietárias foram alteradas ou excluídas.

(fonte: Secretaria de Governo Digital do Ministério da Economia)

c) Recuperabilidade

É preciso, ainda, estabelecer o nível de impacto do incidente nos recursos e o tempo necessário para a recuperação. Nesta etapa identificam-se e avaliam-se os recursos e a importância, para o Tribunal, da recuperação do incidente. As categorias de recuperabilidade estão elencadas dessa forma:

Tabela 4

Categoria	Definição
Regular	O tempo de recuperação é previsível com os recursos existentes.
Suplementado	O tempo de recuperação é previsível com recursos adicionais.
Estendido	O tempo de recuperação é imprevisível; recursos adicionais e ajuda externa são necessários.
Não Recuperável	A recuperação do incidente não é possível (por exemplo, dados confidenciais expostos e postados publicamente); lançar investigação.

(fonte: Secretaria de Governo Digital do Ministério da Economia)
