PORTARIA DG Nº 157, DE 28 DE SETEMBRO DE 2023.

O DIRETOR-GERAL DA SECRETARIA DO TRIBUNAL REGIONAL ELEITORAL DE GOIÁS, no uso de suas atribuições legais e regulamentares,

CONSIDERANDO a necessidade de apoiar a gestão de incidentes de segurança da informação do TRE-GO;

CONSIDERANDO a Res. CNJ 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Res. TSE 23.644/2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a Resolução DG/TSE nº 444/2021, que dispõe sobre a instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior 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 em gestão de incidentes de segurança da informação previstas nas normas ABNT ISO/IEC 27035 (1, 2 e 3);

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

CONSIDERANDO a necessidade de gerenciar os incidentes de segurança da informação que envolvam dados pessoais, de acordo com a lei 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 de Goiás;

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 de Goiás.

CONSIDERANDO a instrução do procedimento administrativo SEI nº 22.0.000013811-1.

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída e regulamentada a gestão de incidentes de segurança da informação no âmbito da Justiça Eleitoral de Goiás.

Art. 2º Esta norma visa atender às orientações fixadas aos Tribunais Regionais Eleitorais previstas na Política de Segurança de Informação da Justiça Eleitoral, estabelecida pelo Tribunal Superior Eleitoral.

Art. 3º Ficam descritas 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, conforme trâmite previsto no fluxograma do Anexo II.

Art. 4º O ciclo de gestão de incidentes de segurança da informação no TRE-GO 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), instituídos no âmbito do TRE-GO, e ainda, em consonância com a Política de Segurança Cibernética do Poder Judiciário (PSEC-PJ), instituída pelo Conselho Nacional de Justiça (CNJ).

CAPÍTULO II
DAS RESPONSABILIDADES

Art. 6º A atuação operacional na resposta a incidentes é de responsabilidade da ETIR (Equipe Técnica de Respostas a Incidentes de Redes Computacionais e Segurança Cibernética).

Art. 7º 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 III

DA PREPARAÇÃO

Art. 8º A ETIR utilizará o seu processo de trabalho e planos de resposta a incidentes, 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. 9º A STI manterá registro de logs de eventos, de acordo com norma específica, com intuito de subsidiar a detecção manual ou automatizada de incidentes.

Art. 10 A unidade de segurança cibernética da STI do TRE-GO monitorará as ameaças cibernéticas em conjunto com as unidades técnicas responsáveis, incluindo o acompanhamento de boletins encaminhados pelo CTIR GOV.

CAPÍTULO IV
DA DETECÇÃO E ANÁLISE

Art. 11 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 meio do monitoramento dos operadores técnicos.

Art. 12 Detectado o incidente ou a suspeita dele, a área técnica responsável pelo ativo de informação atingido acionará a ETIR que fará o registro do incidente e a 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 no negócio e a urgência de sua resolução.

Parágrafo único. A categorização e a priorização do tratamento de incidentes tem como referência o disposto no Anexo I desta norma.

Art. 13 Confirmada a ocorrência do incidente, a ETIR acionará o plano de respostas adequado e comunicará ao Comitê Gestor de Segurança da Informação e, se for o caso, ao Encarregado de Dados Pessoais.

Art. 14 As áreas técnicas envolvidas na resposta ao incidente devem atuar na preservação das evidências forenses para eventual análise posterior, conforme previsto no Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ), destacando-se:

I - efetuar cópia completa do sistema comprometido;

II - efetuar cópias dos logs de acesso;

III - efetuar cópias de mensagens ou arquivos.

Parágrafo único. As áreas técnicas envolvidas na resposta ao incidente farão constar em relatório a eventual impossibilidade de preservação das evidências e listar os procedimentos adotados.

Art. 15 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 no âmbito do Poder Judiciário (Resolução CNJ nº 396 de 07/06/2021), sem prejuízo de outras ações que possam ser identificadas pelo Comitê de Crises Cibernéticas e/ou pela ETIR.

CAPÍTULO V
DA CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO

Art. 16 Após a fase de detecção e análise, a ETIR atuará na localização da causa raiz e na contenção da ameaça, além de promover a recuperação dos ativos.

Art. 17 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 constatação 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.

§ 3º Em caso de incidente grave, a recuperação do ambiente deve ocorrer somente com aval da Chefia do Comitê de Crises nomeado nos termos do Protocolo de Gerenciamento de Crises Cibernéticas.

CAPÍTULO VI
DA AVALIAÇÃO PÓS-INCIDENTE

Art. 18 Concluídas as etapas de tratamento do incidente, a ETIR deverá documentar os procedimentos realizados e as lições aprendidas, por meio de relatório de incidente.

Art. 19 O armazenamento dos relatórios de incidentes terá seu acesso permitido conforme classificação de documentos estabelecida pela Presidência do TRE-GO.

Art. 20 Caso não seja possível determinar adequadamente a causa raiz, a ETIR deverá registrar como problema para análise posterior.

CAPÍTULO VII
DA COMUNICAÇÃO

Art. 21 Em caso de incidente que possa acarretar dano relevante para titulares de dados pessoais controlados pelo TRE-GO, o Encarregado de Dados Pessoais realizará a comunicação à Presidência do Tribunal, à ANPD e aos titulares de dados.

Parágrafo único. Cabe ao Encarregado de Dados Pessoais juntamente com a Assessoria de Imprensa e Comunicação Social, elaborar o teor do comunicado aos titulares de dados afetados pelo incidente.

Art. 22 O Agente Responsável pela ETIR encaminhará ao Gestor de Segurança da Informação e ao Encarregado de Dados Pessoais relatório resumido de todos os incidentes categorizados como graves que envolvam dados pessoais, tão logo a gravidade do incidente seja definida.

Art. 23 O Gestor de Segurança da Informação apresentará ao CGSI, ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ) e à ETIR do TSE as informações relevantes acerca dos incidentes graves ocorridos.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS

Art. 24 Os casos omissos serão resolvidos pelo Comitê Gestor de Segurança da Informação ou pelo Comitê Gestor de Proteção de Dados Pessoais, de acordo com o tipo do incidente.

Art. 25 Esta norma deve ser revisada a cada 3 anos, ou antes, se necessário, pelo Comitê Gestor de Segurança da Informação.

Art. 26 Esta norma deve ser publicada no portal de internet do Tribunal pelo Comitê Gestor de Segurança da Informação.

Art. 27 Esta Portaria entra em vigor na data de sua publicação.

Wilson Gamboge Júnior
Diretor-Geral

ANEXO I – Categorização e priorização 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: *fingerid*, 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	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 ilegais ou esquemas de pirâmide).
	Direitos autorais (*copyright*)	Vender ou instalar cópias de *software* ou outros materiais protegidos por direitos autorais sem a devida licença.
	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 – Níveis de Impacto no Negócio

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 – Categorias de Impacto

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

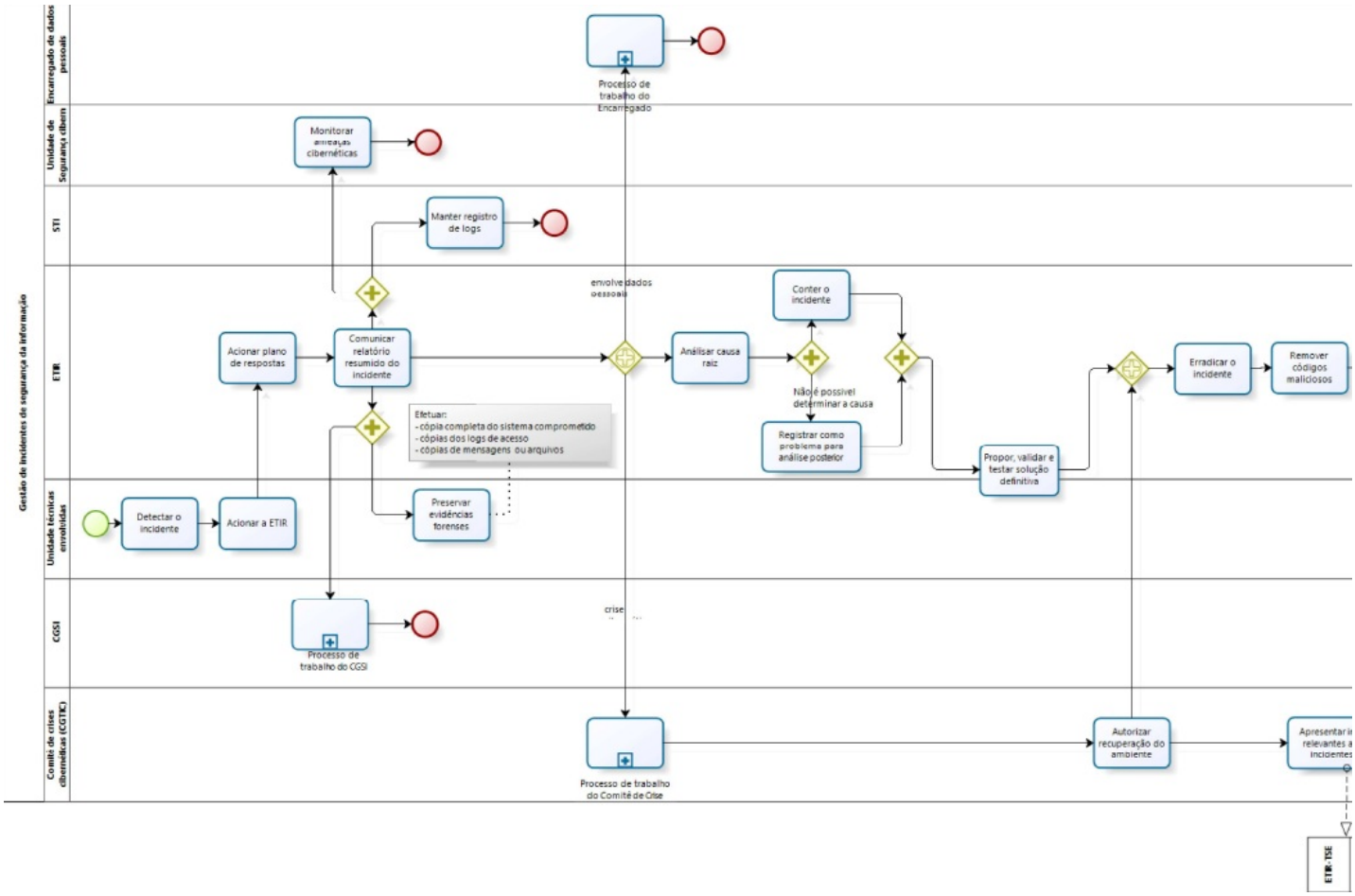
É preciso, ainda, estabelecer o nível do incidente nos recursos e o tempo necessário para a recuperação. Nesta etapa identificam-se e avaliam-se os recursos e a importância, para o Tribunal, da recuperação do incidente. As categorias de recuperabilidade estão elencadas dessa forma:

Tabela 4 – Categorias de Recuperabilidade

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)

ANEXO II – Fluxograma


Gestão de incidentes de segurança da informação
Encarregado de dados pessoais
Unidade de Segurança cibern
STI
ETIR
Unidade técnicas envolvidas
CGSI
Comitê de crises cibernéticas (CGTIC)
Processo de trabalho do Encarregado
Monitorar ameaças cibernéticas
Manter registro de logs
envolve dados pessoais
Conter o incidente
Acionar plano de respostas
Comunicar relatório resumido do incidente
Analisar causa raiz
Não é possível determinar a causa
Registrar como problema para análise posterior
Propor, validar e testar solução definitiva
Erradicar o incidente
Remover códigos maliciosos
Efetuar:
- cópia completa do sistema comprometido
- cópias dos logs de acesso
- cópias de mensagens ou arquivos
Detectar o incidente
Acionar a ETIR
Preservar evidências forenses
crise
Processo de trabalho do CGSI
Processo de trabalho do Comitê de Crise
Autorizar recuperação do ambiente
ETIR-TSE