INSTRUÇÕES NORMATIVAS

INSTRUÇÃO NORMATIVA TRE-RS P N. 101/2023

DISPÕE SOBRE A INSTITUIÇÃO DA GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de apoiar a gestão de incidentes de segurança da informação do Tribunal Regional Eleitoral do Rio Grande do Sul;

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

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

CONSIDERANDO a Resolução TRE-RS 370/2021, que adota, no âmbito do Tribunal, a Resolução TSE 23.644/2021;

CONSIDERANDO a Resolução TRE-RS 401/2022, que institui a Política da Continuidade de Negócios no âmbito do Tribunal Regional Eleitoral do Rio Grande do Sul;

CONSIDERANDO a Portaria DG/TSE 444/2021, que dispõe sobre a instituição da norma de termos e definições relativas 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 a necessidade de gerenciar os incidentes de segurança da informação que envolvam dados pessoais, de acordo com a Lei 13.709/2018 (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 Grande do Sul;

RESOLVE:

Art. 1° Instituir a Gestão de Incidentes de Segurança da Informação como norma integrante da Política de Segurança de Informação da Justiça Eleitoral, estabelecida pela Resolução TSE 23.644 /2021.

CAPÍTULO I

DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para efeitos desta norma consideram-se os termos e definições previstos na Portaria TSE 444/2021, além dos seguintes:

I - ANPD: acrônimo de Autoridade Nacional de Proteção de Dados Pessoais;

II - crise: situação considerada quando os impactos de incidentes cibernéticos, ou de outra natureza, possam caracterizar grave dano material ou de imagem; ou quando restar evidente que as ações de resposta ao incidente se estenderão por dias, semanas ou meses; ou o incidente impactar a atividade finalística ou o serviço crítico; ou, ainda, o incidente atrair grande atenção da mídia e da população em geral;

III - CTIR GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal;

IV - ETIR (Equipe Técnica de Respostas a Incidentes em Redes Computacionais): grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

V - evento de segurança: qualquer ocorrência identificada em um sistema, serviço ou rede que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida que possa se tornar relevante em termos de segurança;
VI - 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;
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 II

DAS DISPOSIÇÕES GERAIS

Art. 3º Esta norma tem como objetivo estabelecer diretrizes para as estratégias de gestão de incidentes de segurança da informação, que envolvam ou não dados pessoais, permitindo a adequada preparação, detecção, contenção, erradicação, recuperação, avaliação e comunicação no tratamento de incidentes.

Parágrafo único. A gestão de incidentes visa proteger a organização, minimizando os impactos causados por incidentes e apoiando a recuperação rápida do ambiente.

CAPÍTULO III

DAS RESPONSABILIDADES

Art. 4° Cabe à ETIR:
I - atuar operacionalmente na resposta a incidentes;
II - monitorar ameaças cibernéticas, incluindo o acompanhamento de boletins encaminhados pelo CTIR GOV;
III - elaborar e manter o Plano de Resposta a Incidentes.

Parágrafo único. O Plano de Resposta a Incidentes deverá conter as estratégias de contenção, erradicação e recuperação e os meios de comunicação oficiais e adicionais a serem acionados durante os procedimentos de resposta específicos.

Art. 5° Cabe à Secretaria de Tecnologia da Informação manter registro de eventos (log), de acordo com norma específica, com intuito de subsidiar a detecção manual ou automatizada de incidentes.

Art. 6° Em situações declaradas como crise, cabe ao Comitê de Pronta Resposta determinar as providências cabíveis para o seu enfrentamento.

Art. 7° Todas as pessoas que utilizam os ativos de informação deste Tribunal são corresponsáveis pela segurança da informação, cabendo-lhes a comunicação imediata, por meio dos canais próprios fornecidos pela Secretaria de Tecnologia da Informação, de qualquer evento de segurança de que tenham conhecimento.

Art. 8° Cabe ao Comitê de Segurança da Informação e Proteção de Dados Pessoais (CSI) o monitoramento das atividades da ETIR e o estabelecimento de métricas de desempenho.

Art. 9° Cabe ao serviço de Help Desk receber e categorizar os eventos de segurança relatados por usuários e usuárias internos ou externos, escalonando para ETIR aqueles que forem detectados como possíveis incidentes de segurança, caso necessário.

CAPÍTULO IV

DA DETECÇÃO E ANÁLISE

Art. 10. A detecção dos eventos de segurança poderá ocorrer de forma proativa, através de sistemas de detecção e prevenção de intrusões e ferramentas automatizadas ou manuais de monitoramento, ou de forma reativa, por comunicação de usuários e usuárias internos ou externos.
Parágrafo único. Os eventos de segurança deverão ser registrados e encaminhados à ETIR para análise.
Art. 11. A ETIR verificará se o evento se trata de um incidente em potencial e promoverá a sua classificação, categorização, correlação e priorização.
§ 1° Os incidentes devem ser classificados de acordo com a importância ou prioridade das informações e sistemas de informação, impacto nos negócios, escala de danos e gravidade.
§ 2° A priorização do incidente deverá considerar, no mínimo, o seguinte:
I - impacto na imagem da Instituição reputação;
II - proteção de informações confidenciais e dados pessoais;
III - ameaça à infraestrutura crítica;
IV - paradas ou danos nas operações.
Art. 12. A ETIR realizará a análise do incidente e sua correlação com outros anteriormente registrados.
Art. 13. As evidências do incidente devem ser preservadas para futura referência ou para procedimentos disciplinares ou legais.
§ 1° A preservação das evidências deve respeitar a cadeia de custódia.
§ 2° Os dados coletados, como arquivos com o registro de eventos (log), informação sobre processos, status de conexão de rede, conteúdo de arquivos, softwares maliciosos, banco de dados etc., devem ser escritos em uma imagem, como a exportação de um banco de dados, arquivo de histórico, captura de tela, imagem de disco, ente outros.
CAPÍTULO V
DA CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO
Art. 14. A ETIR promoverá a resposta aos incidentes ocorridos ou em andamento, por meio da contenção, erradicação e recuperação, com o objetivo de:
I - parar ou minimizar os efeitos ou danos do ataque, mantendo a continuidade da missão operacional;
II - assegurar a recuperação efetiva e oportuna dos sistemas, de forma a prevenir que incidentes semelhantes ocorram novamente;
III - reforçar a postura defensiva e a prontidão operacional da organização;
IV - assegurar que atividades de resposta ocorram de uma maneira que protejam quaisquer dados, de acordo com o seu nível de sensibilidade;
V - oferecer apoio à caracterização rápida e completa de ataques;
VI - desenvolver e implementar cursos de ação;
VII - remediar ou mitigar a atividade;
VIII - recuperar os sistemas para o nível operacional normal;
IX - melhorar os processos de infraestrutura e de tratamento de incidentes.
Parágrafo único. Antes da execução do procedimento de resposta específico, devem ser coletados todos os dados necessários para a análise e preservação das evidências.
CAPÍTULO VI
DA GERAÇÃO DE RELATÓRIOS DE INCIDENTES
Art. 15. O incidente deve ser registrado, especificando quais foram os procedimentos de resposta utilizados para contorná-lo, de forma a manter um histórico das ocorrências e das ações tomadas, considerando o nível de classificação da informação quanto a sua confidencialidade.
Parágrafo único. Registros de incidentes classificados como graves devem ter seu acesso restrito.

Art. 16. A ETIR deverá encaminhar ao Gestor de Segurança da Informação relatório mensal com todos os incidentes ocorridos.
Art. 17. O Agente Responsável pela ETIR encaminhará ao Gestor de Segurança da Informação relatório de todos os incidentes categorizados como graves, tão logo a gravidade do incidente seja definida.
Art. 18. O Agente Responsável pela ETIR encaminhará ao Encarregado de Dados Pessoais relatório de todos os incidentes que envolvam dados pessoais.
CAPÍTULO VII
DA COMUNICAÇÃO
Art. 19. O Gestor de Segurança da Informação apresentará ao CSI e à ETIR do Tribunal Superior Eleitoral as informações relevantes acerca dos incidentes graves ocorridos.
Art. 20. Na ocorrência de incidente de segurança que acarrete risco ou dano relevante aos titulares dos dados, o Encarregado de Dados Pessoais fará a comunicação do incidente, no prazo de até 72 horas, à Autoridade Nacional de Proteção de Dados (ANPD), ao Tribunal Superior Eleitoral e aos titulares dos dados. (IN TRE-RS P N. 93/2022.)
Art. 21. Em casos declarados como crise, cabe ao Comitê de Pronta Resposta a comunicação interna e externa do incidente.
CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS
Art. 22. Os casos omissos serão resolvidos pela Diretoria-Geral, ouvido o Comitê de Segurança da Informação e Proteção de Dados Pessoais.
Art. 23. O descumprimento não fundamentado desta norma deve ser comunicado e registrado pelo Gestor de Segurança da Informação, com consequente adoção das providências cabíveis.
Art. 24. Esta Instrução Normativa entra em vigor na data de sua publicação e sua implementação inicia-se imediatamente.
DESEMBARGADOR FRANCISCO JOSÉ MOESCH,
PRESIDENTE.

PORTARIAS

PORTARIA TRE-RS P N. 1619, DE 14 DE FEVEREIRO DE 2023.

O DESEMBARGADOR FRANCISCO JOSÉ MOESCH, PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL, NO USO DE SUAS ATRIBUIÇÕES LEGAIS, EM CONFORMIDADE COM O ART. 36, INCISO III, ALÍNEA "B", DA LEI N. 8.112/1990, COM OS ARTS. 5º E 19 DA RESOLUÇÃO TSE N. 23.563/2018 E COM A DECISÃO PROFERIDA NOS AUTOS DO PROCESSO N. 0016902-59.2022.6.21.8054,
RESOLVE,
Art. 1º REMOVER, por motivo de saúde, pelo prazo de 12 (doze) meses, a contar de 22 de fevereiro de 2023, a servidora CARLA REGINA HEPP, ocupante do cargo de Técnico Judiciário, Área Administrativa, do Quadro de Pessoal deste Tribunal, para o município de Lajeado/RS, de acordo com o laudo de Inspeção de Saúde emitido pela Junta Médica deste Tribunal.
Art. 2º Esta Portaria entra em vigor na data de sua publicação.
DESEMBARGADOR FRANCISCO JOSÉ MOESCH,
PRESIDENTE.

PORTARIA TRE-RS P N. 1618, DE 14 DE FEVEREIRO DE 2023.

O DESEMBARGADOR FRANCISCO JOSÉ MOESCH, PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL, NO USO DE SUAS ATRIBUIÇÕES LEGAIS E