PRESIDÊNCIA

PORTARIAS

PORTARIA N.º 355/2022

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO PARANÁ, usando das atribuições que lhe são conferidas pelo artigo 23, inciso XXXIII, do Regimento Interno deste Tribunal, considerando o PAD nº 4847/2022, considerando o programa "Cidadania Plena" instituído pela Portaria nº 186/2022, e o disposto em seu art. 5º,

RESOLVE

Art. 1º DESIGNAR os servidores abaixo nominados para, sob a coordenação da Drª. LUCIANI DE LOURDES TESSEROLI MARONEZI, comporem a COMISSÃO RELATIVA AO PROGRAMA CIDADANIA PLENA NO ÂMBITO DA JUSTIÇA ELEITORAL DO PARANÁ:

I- CLAUDEMIR PEREIRA DE CARVALHO, Chefe de Cartório da 3ª Zona Eleitoral de Curitiba;

II- CLAUDIA AFANIO, Coordenadora de Inovação e Sustentabilidade;

III- DESIREE HERNANDEZ MAUSBACH RICCO, Coordenadora de Sistemas;

IV- DIOGO SGUISSARDI MARGARIDA, Coordenador de Planejamento de Estratégia e Gestão;

V- JOSMAR AMBRUS, Secretário da Presidência;

VI- MARDEN LINCOLN AMARAL MACHADO, Secretário de Comunicação Social;

VII- MARIA ANGELA DE OLIVEIRA, Assistente III do Laboratório de Inovação, Inteligência e Objetivos de Desenvolvimento Sustentável;

VIII- PATRICIA GASPARRO SEVILHA GRECO, Chefe de Cartório da 66ª Zona Eleitoral de Maringá;

IX- PAULO CEZAR RIBEIRO, Chefe de Cartório da 156ª Zona Eleitoral de Rio Branco do Sul;

X- SOLANGE MARIA VIEIRA, Secretária de Planejamento e Logística de Eleições e Inovação;

XI- WILLIAN GALLERA GARCIA, Coordenador de Planejamento de Eleições.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

Curitiba, 12 de setembro de 2022.

Des. COIMBRA DE MOURA

Presidente

DIRETORIA-GERAL

INSTRUÇÃO NORMATIVA

INSTRUÇÃO NORMATIVA Nº 02/2022

Dispõe sobre as regras e os procedimentos para gestão de incidentes de segurança da informação no âmbito da Justiça Eleitoral do Paraná.

O DIRETOR-GERAL DA SECRETARIA DO TRIBUNAL REGIONAL ELEITORAL DO PARANÁ, no uso das atribuições que lhe são conferidas pelo inciso VII do art. 29 do Regulamento da Secretaria (Resolução TRE-PR nº 878/2021),

CONSIDERANDO a necessidade de aprimorar e regulamentar a gestão de incidentes de segurança da informação do TRE-PR;

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

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

CONSIDERANDO a Portaria 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 nº 13.709/2018 (Lei Geral de Proteção de Dados);

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 Paraná; e,

CONSIDERANDO o contido no PAD nº 25959/2022,

RESOLVE

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º A presente norma institui e regulamenta a gestão de incidentes de segurança da informação no âmbito da Justiça Eleitoral do Paraná.

Art. 2º 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.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 3º Para efeitos desta norma, consideram-se os termos e as definições previstas na Portaria DG /TSE nº 444/2021, além dos seguintes:

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 Técnica de Respostas a Incidentes de Redes Computacionais) - 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, entre outros;

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, 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 - 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 normativo próprio;

IX - 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. 4º A atuação operacional na resposta a incidentes é de responsabilidade da ETIR (Equipe Técnica de Respostas a Incidentes de Redes Computacionais), que será nomeada em portaria específica.

Art. 5º A comunicação externa com a ANDP e com os titulares de dados, em caso de incidentes graves envolvendo dados pessoais é de responsabilidade do Encarregado de Dados Pessoais.

Art. 6º A comunicação externa com a sociedade, em caso de incidentes graves, que inviabilizem as atividades precípuas do TRE-PR, por prazo maior que o Objetivo de Tempo de Recuperação (OTR /RTO), é do Gestor de Crises, nomeado em portaria específica, ou outra autoridade determinada pela Presidência do TRE-PR.

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 disponibilizados pela SECTI.

Art. 8º Cabe a Secretaria de Tecnologia da Informação o monitoramento das atividades da ETIR e o estabelecimento de métricas de desempenho.

CAPÍTULO IV

DA PREPARAÇÃO

Art. 9º A ETIR elaborará o seu processo de trabalho e planos de resposta à 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. 10. A SECTI manterá registro de logs de eventos, de acordo com norma específica, com intuito de subsidiar a detecção manual ou automatizada de incidentes.

Art. 11. A ETIR determinará os meios de comunicação oficiais e adicionais a serem acionados durante o processo de resposta à incidentes.

Art. 12. A ETIR fará o monitoramento de ameaças cibernéticas, incluindo o acompanhamento de boletins encaminhados pelo CTIR GOV.

CAPÍTULO V

DA DETECÇÃO E DA 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 ou através de comunicação de usuários.

Art. 14. Detectado o incidente ou a suspeita dele, a ETIR fará o registro do incidente, acionará o plano de resposta adequado e encaminhará para análise das áreas responsáveis.

Art. 15. Confirmada a ocorrência do incidente, a ETIR acionará o plano de respostas adequado.

Art. 16. As áreas técnicas envolvidas na resposta ao incidente devem, na medida do possível, atuar para preservar as evidências forenses para eventual análise posterior, como:

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.
CAPÍTULO VI
DA CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO
Art. 17. 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.
Art. 18. 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 tratados.
Art. 19. 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-PR.
CAPÍTULO VII
DA AVALIAÇÃO PÓS-INCIDENTE
Art. 20. 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. 21. O armazenamento dos relatórios de incidentes deverá ocorrer em sistema de informação específico, tendo seu acesso restrito.
Art. 22. Caso a causa raiz não possa ser adequadamente determinada, a ETIR deverá registrar como problema para análise posterior.
CAPÍTULO VIII
DA COMUNICAÇÃO
Art. 23. 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 o incidente seja encerrado.
Art. 24. O Gestor de Segurança da Informação apresentará ao CGSI as informações relevantes acerca dos incidentes graves ocorridos.
Art. 25. 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.
CAPÍTULO IX
DAS DISPOSIÇÕES FINAIS
Art. 26. O descumprimento não fundamentado desta norma deve ser comunicado e registrado pelo Gestor de Segurança da Informação, com consequente adoção das providências cabíveis.
Art. 27. Esta norma deve ser revisada a cada 12 (doze) meses, ou antes, caso necessário, pelo Gestor de Segurança da Informação e encaminhada para apreciação do Comitê Gestor de Segurança da Informação (CGSI).
Art. 28. 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. 29. Esta instrução normativa entra em vigor na data de sua publicação.
Curitiba, em 30 de agosto de 2022.
VALCIR MOMBACH
Diretor-Geral do TRE-PR

INSTRUÇÃO NORMATIVA 03/2022

Dispõe sobre as regras e os procedimentos para a realização da gestão e monitoramento de registro de atividades (logs) no ambiente computacional da Justiça Eleitoral do Paraná.