RESOLVE:
Art. 1º Fica instituído Plano de Resposta a Incidentes do Tribunal Regional Eleitoral do Amazonas.
Art. 2º Esta norma integra a Política de Segurança da Informação da Justiça Eleitoral, estabelecida pela Resolução TSE n. 23.644/2021.
Art. 3º Determinar sua observância em todo âmbito do Tribunal Regional Eleitoral do Amazonas.
Art. 4º Qualquer descumprimento desta norma deve ser imediatamente comunicado e registrado pelo Gestor de Segurança da Informação, com consequente adoção das providências cabíveis.
Art. 5º Esta norma complementar deverá ser revisada a cada 12 meses pelo Gestor de Segurança da Informação e encaminhada para nova apreciação do Comitê de Segurança da Informação e de Gerenciamento de Crises Cibernéticas.
Art. 6º Esta Política deve ser publicada no portal de intranet do Tribunal pelo Comitê de Segurança da Informação.
Art. 7º Esta Portaria entra em vigor na data de sua publicação.
Desembargador JORGE MANOEL LOPES LINS
Presidente do TRE - AM

PORTARIA Nº 198, DE 10 DE ABRIL DE 2023

O PRESIDENTE DO EGRÉGIO TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS, no uso das competências que lhe são conferidas pelo art. 18, incisos XII, do Regimento Interno e com fundamento no art. 35, inciso I, da Lei n. 8.112, de 11.12.1990, com redação dada pela Lei n. 9.527, de 10.12.1997,
CONSIDERANDO a Res. CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO a Res. 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 instituiu a norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral;
CONSIDERANDO as boas práticas de segurança da informação e privacidade previstas nas normas ABNT ISO/IEC 27001 e ABNT ISO/IEC 27002;
CONSIDERANDO as boas práticas em gestão de riscos de segurança da informação previstas na 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 o tratamento de dados pessoais, de acordo com a lei 13.709/2018 (LGPD);
CONSIDERANDO, ainda, que a segurança da informação, a proteção e privacidade de dados pessoais são condições essenciais para a prestação dos serviços jurisdicionais e administrativos do Tribunal Regional Eleitoral Amazonas;
RESOLVE:
CAPÍTULO I
DISPOSIÇÕES PRELIMINARES
Art. 1º Fica instituída a Instrução Normativa para a Gestão de Incidentes de Segurança da Informação no âmbito do Tribunal Regional Eleitoral Amazonas.
Art. 2º Esta norma integra a Política de Segurança da Informação da Justiça Eleitoral, estabelecida pela Resolução TSE n. 23.644/2021.
CAPÍTULO II
DAS DEFINIÇÕES

Art. 3º Para efeitos desta norma, consideram-se os termos e definições previstos na Portaria DG /TSE n. 444/2021, além das 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 de Tratamento e Resposta a Incidentes de Segurança Cibernética.

IV. CSIGCC: Comitê de Segurança da Informação e de Gerenciamento de Crises Cibernéticas.

V. 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.

VI. Incidente de segurança da informação: Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de informação ou das redes de computadores.

VII. Incidente de segurança da informação envolvendo 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.

VIII. 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.

IX. 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.

X. 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.

Art. 4º 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 III

DAS RESPONSABILIDADES

Art. 5º A atuação operacional na resposta a incidentes, no âmbito do TRE-AM, é de responsabilidade da ETIR.

Art. 6º 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 Proteção de Dados Pessoais.

Art. 7º A comunicação externa com a sociedade, em caso de incidentes graves, que inviabilizem as atividades precípuas do TRE-AM por prazo maior que o Objetivo de Tempo de Recuperação (OTR /RTO), é do Gestor de Crises, nomeado em portaria específica, ou por outra autoridade determinada pela presidência do TRE-AM.

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.

Art. 9º Cabe ao CSIGCC o monitoramento das atividades da ETIR e o estabelecimento de métricas de desempenho.

CAPÍTULO IV

DA PREPARAÇÃO

Art. 10º A ETIR elaborará o seu processo de trabalho e plano 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. 11º 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. 12º A ETIR determinará os meios de comunicação oficiais e adicionais a serem acionados durante o processo de resposta à incidentes.

Art. 13º A ETIR fará o monitoramento de ameaças cibernéticas, incluindo o acompanhamento de boletins encaminhados pelo CTIR GOV.

CAPÍTULO V

DA DETECÇÃO E ANÁLISE

Art. 14º 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. 15º Detectado o incidente ou a suspeita dele, a área técnica responsável pelo ativo de informação atingido, ou a ETIR, farão o registro do incidente para análise.

Art. 16º Confirmada a ocorrência do incidente, a ETIR acionará o plano de respostas adequado.

Art. 17º 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. 18º 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. 19º 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. 20º 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-AM.

CAPÍTULO VII

DA AVALIAÇÃO PÓS-INCIDENTE

Art. 21º Os 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. 22º Art. 22. O armazenamento dos relatórios de incidentes deverá ocorrer em sistema de informação específico, tendo seu acesso restrito.

Art. 23º Art. 23. Caso a causa raiz não possa ser adequadamente determinada, a ETIR deverá registrar como problema para análise posterior.

CAPÍTULO VIII

DA COMUNICAÇÃO

Art. 24º 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. 25º O Gestor de Segurança da Informação apresentará ao CSIGCC e à ETIR do TSE as informações relevantes acerca dos incidentes graves ocorridos.

Art. 26º 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
DISPOSIÇÕES FINAIS
Art. 27º Os casos omissos serão resolvidos pelo Comitê de Segurança da Informação e de Gerenciamento de Crises Cibernéticas ou pelo Comitê Gestor de Proteção e Privacidade de Dados Pessoais, de acordo com o tipo do incidente.
Art. 28º Qualquer descumprimento desta norma deve ser imediatamente comunicado e registrado pelo Gestor de Segurança da Informação, com consequente adoção das providências cabíveis.
Art. 29º Esta norma complementar deverá ser revisada a cada 12 meses pelo Gestor de Segurança da Informação e encaminhada para nova apreciação do Comitê de Segurança da Informação e de Gerenciamento de Crises Cibernéticas.
Art. 30º Esta Política deve ser publicada no portal de intranet do Tribunal pelo Comitê de Segurança da Informação.
Art. 31º Esta Portaria entra em vigor na data de sua publicação.
Desembargador JORGE MANOEL LOPES LINS
Presidente do TRE - AM

PORTARIA Nº 431, DE 2 DE MAIO DE 2023

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS, considerando a Resolução CNJ nº 343, de 09 de setembro de 2020, que regulamenta o teletrabalho, sob condições especiais, no âmbito do Poder Judiciário c/c Resolução TRE/AM Nº 12, de 21 de janeiro de 2021, que define condições especiais para concessão de teletrabalho, no âmbito do Tribunal Regional Eleitoral do Amazonas, bem como o teor do Processo Eletrônico - SEI n. 3000-85.2023.6.04.0000,
RESOLVE:
Art. 1º Fica concedido o regime de teletrabalho especial ao servidor MARCELO DOS SANTOS REGO, Técnico Judiciário - Área Administrativa, Matrícula 2.301.742, pelo período de 29/05/2023 a 29/11/2023.
Art. 2º Esta Portaria entra em vigor na data de sua publicação.
Desembargador JORGE MANOEL LOPES LINS
Presidente do TRE/AM

PORTARIA Nº 367, DE 17 DE ABRIL DE 2023

O PRESIDENTE DO EGRÉGIO TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS, no uso das competências que lhe são conferidas pelo art. 18, incisos XII, do Regimento Interno e com fundamento no art. 35, inciso I, da Lei n. 8.112, de 11.12.1990, com redação dada pela Lei n. 9.527, de 10.12.1997,
CONSIDERANDO o art. 37, § 6º da Constituição Federal, que dispõe sobre a responsabildiade objetiva atribuída aos entes estatais;
CONSIDERANDO a Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO a Resolução 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 instituiu a norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral;
CONSIDERANDO o disposto na Resolução TSE nº 23.387/2012, que dispõe sobre o uso da rede corporativa de comunicação de dados na Justiça Eleitoral;;
CONSIDERANDO o disposto na Portaria TSE nº 456/2021, que dispões sobre o uso aceitável de ativos de TI;