# PORTARIA N° 146, DE 08 DE ABRIL DE 2021.

**Institui o modelo de implementação da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) no âmbito do TRE/AM.**

**O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS**, no uso das suas atribuições legais e regimentais e,

**CONSIDERANDO** a importância da adoção de boas práticas relacionadas à proteção da informação preconizadas pelas normas ISO NBR/IEC 27001:2013 e 27002:2013;

**CONSIDERANDO** a Política de Segurança da Informação do TRE/AM, aprovada pela Portaria TRE/AM n° 600/2019;

**CONSIDERANDO** a Portaria TRE/AM n° 399/2020, que institui a Comissão de Segurança da Informação do TRE/AM para o biênio 2020-2022, especialmente o art. 9º, que conferiu à referida Comissão a inciativa de propor o modelo de implementação da Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais (ETIR), de acordo com a norma vigente;

**CONSIDERANDO** a Resolução/CNJ nº 360/2020 - Determina a adoção do Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Poder Judiciário (PGCC/PJ);

**CONSIDERANDO** a Resolução/CNJ nº 361/2020 - Determina a adoção de Protocolo de Prevenção a Incidentes Cibernéticos no âmbito do Poder Judiciário (PPICiber/PJ);

**CONSIDERANDO** a Resolução/CNJ nº 362/2020 - Institui o Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário (PGCC/ PJ);

**CONSIDERANDO** a Portaria CNJ n° 290, de 17 de dezembro de 2020, que institui o Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Poder Judiciário (PGCC/ PJ), enfatizando que o tratamento de incidentes cibernéticos não mais se restringe a área de tecnologia da informação (art. 4º, inciso IX);

**CONSIDERANDO** a Portaria CNJ n° 291, de 17 de dezembro de 2020, que Institui o Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário;

**CONSIDERANDO** a Portaria CNJ n° 292, de 17 de dezembro de 2020, que determina a adoção de Protocolo de Prevenção a Incidentes Cibernéticos no âmbito do Poder Judiciário (PPICiber/PJ,

**RESOLVE**

**Art. 1º Instituir** a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética – ETIR, segundo o modelo de implementação estabelecido nesta Portaria.

## CAPÍTULO I

**TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS**

**DO OBJETIVO**

**Art. 2º** A **ETIR**, no âmbito do Tribunal Regional Eleitoral do Amazonas, tem como objetivo garantir o cumprimento da missão institucional do Tribunal Regional Eleitoral do Amazonas TRE/AM por meio do tratamento e resposta a incidentes de segurança cibernética.

## CAPÍTULO II

## DA COMPOSIÇÃO

**Art. 3º** A **ETIR** terá como membros os titulares das unidades abaixo relacionadas ou seus respectivos substitutos legais, em caso de afastamentos daqueles:

- Coordenadoria de Infraestrutura – COINF;
- Seção de Rede e Banco de Dados - SERBD;
- Seção de Produção – SEPD;
- Coordenadoria de Desenvolvimento de Sistemas- CDES;
- Assessoria de Comunicação Social - ASCOM;
- Coordenadoria de Registros e Editoração – CORE;
- Núcleo de Apoio de Segurança Judiciária - NASJ; e
- Coordenadoria de Controle Interno e Auditoria- CCIA.

**§ 1**° Dentre os titulares constantes no *caput*, o Coordenador de Infraestrutura atuará como **Agente Responsável**.

**Art. 4º** A ETIR funcionará como um grupo de trabalho permanente de atuação primordialmente reativa e não exclusiva.

**Parágrafo Único.** As atividades reativas da ETIR terão prioridade sobre aquelas designadas pelos chefes imediatos das unidades de seus integrantes.

## CAPÍTULO III

## DOS SERVIÇOS E PROCEDIMENTOS

**Art. 5º** São serviços a serem implementados e desempenhados pela ETIR:

**I.** Tratamento e resposta a Incidentes de Segurança Cibernética;

**II.** Tratamento de artefatos maliciosos;

**III.** Tratamento de vulnerabilidades;

**IV.** Monitoramento da segurança cibernética;

**V.** Análise dos processos e procedimentos utilizados pela ETIR;

**VI.** Prospecção ou monitoração de novas tecnologias;

**VII.** Registro dos incidentes de segurança cibernética notificados ou detectados, com o objetivo de assegurar registro histórico das atividades da ETIR;

**VIII.** Emissão de alertas e advertências;

**IX.** Anúncios - divulgação de forma proativa;

**X.** Avaliação de segurança cibernética;

**XI.** Detecção de intrusão;

**XII.** Disseminação de informações relacionadas à segurança;

**XIII.** Análise crítica sobre os registros de falhas para assegurar que estas sejam satisfatoriamente resolvidas;

**XIV.** Implementação de mecanismos para permitir a quantificação e monitoração dos tipos, volumes e custos de incidentes e falhas de funcionamento;

**XV.** Recolhimento de evidências imediatamente após a constatação de um incidente de segurança da informação na rede interna de computadores; e

**XVI.** Indicação da necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências de incidentes.

**Art. 6º** A ETIR, sob a supervisão do seu Agente Responsável, durante o processo de tratamento do incidente penalmente relevante, deverá, sem prejuízo de outras ações, coletar e preservar:

**I.** As mídias de armazenamento dos dispositivos afetados ou as suas respectivas imagens forenses;

**II.** Os dados voláteis armazenados nos dispositivos computacionais, como a memória principal (memória RAM); e

**III.** Todos os registros de eventos citados no Capítulo IV, da Portaria CNJ n°291/2020, que trata de investigação de ilícitos cibernéticos.

**Art. 7º** Nos casos de inviabilidade de preservação das mídias de armazenamento mencionadas no inciso I do art. 6º, em razão da necessidade de pronto restabelecimento do serviço afetado, a ETIR, sob a supervisão do Agente Responsável, deverá coletar e armazenar cópia dos arquivos afetados pelo incidente, tais como: logs, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original e os "metadados" desses arquivos, como data, hora de criação e permissões.

**Parágrafo Único.** O Agente Responsável pela ETIR deverá fazer constar em relatório a eventual impossibilidade de preservação das mídias afetadas e listar todos os procedimentos adotados.

**Art. 8º** Para cada serviço elencado no artigo 5º, deverão ser formalizados procedimentos a serem observados pela ETIR, em documento a ser elaborado pelo Agente Responsável, com o apoio de toda a equipe, contendo os seguintes atributos:

I. A definição do serviço;

II. O objetivo do serviço; e

III. A descrição das funções e procedimentos que compõem o serviço.

## CAPÍTULO IV

## DO PÚBLICO-ALVO

**Art. 9º** A ETIR atenderá, por meio do serviço de registro de chamados na Central de Serviços, a todos os usuários de sistemas do TRE/AM que comunicarem eventos identificados como incidentes de segurança cibernética.

**Parágrafo Único.** Após o registro do incidente, este será encaminhado ao Agente Responsável que tomará as medidas necessárias.

**Art. 10.** A ETIR, no âmbito externo, poderá interagir com outros órgãos da Administração Pública Federal, do Poder Legislativo, do Poder Judiciário e do Ministério Público que atuem no mesmo campo da Equipe, fornecendo informações acerca dos incidentes de segurança cibernética ocorridos no TRE/AM, alimentando as suas bases de conhecimentos e fomentando a troca de tecnologias.

**Parágrafo Único.** A comunicação sobre os incidentes de segurança, bem como o tratamento aplicado, será efetuada por meio de documento formal.

## CAPÍTULO V

## DA AUTONOMIA

**Art. 11**. A ETIR estará vinculada ao Comitê de Segurança da Informação e de Gerenciamento de Crises Cibernéticas do TRE/AM e terá plena autonomia para desenvolver suas atividades.

**§ 1º** Durante um incidente de segurança, a ETIR poderá tomar decisão de execução das medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

**§ 2°** A ETIR deverá apresentar mensalmente ao Comitê de Segurança da Informação e de Gerenciamento de Crises Cibernéticas relatórios estatísticos dos incidentes de segurança ocorridos no período, com os respectivos tratamentos adotados, com vistas à elaboração de estudos de melhoria dos mecanismos de segurança estabelecidos neste Tribunal Regional ou para fins de tomada de decisão estratégica relativa à Segurança da Informação junto à Administração.

## CAPÍTULO VI

## DAS RESPONSABILIDADES DO AGENTE RESPONSÁVEL

**Art. 12.** Caberá ao Agente Responsável:

I. Elaborar os procedimentos internos a serem adotados pela ETIR com apoio da própria equipe, no prazo máximo de 12 (doze) meses e atualiza-los sempre que necessário;

II. Gerenciar as atividades desempenhadas pela ETIR;

**III.** Distribuir, sempre que necessário, tarefas para a ETIR, inclusive as de caráter proativo;

**IV.** Assegurar que os usuários sejam informados sobre os procedimentos adotados em relação aos incidentes de segurança da informação por eles comunicados;

**V.** Zelar pela capacitação dos membros da ETIR, fazendo constar do Plano Anual de Capacitação os eventos que entender relevantes ao bom desempenho dos trabalhos da equipe;

**VI.** Apoiar a ETIR na execução de seu trabalho, viabilizando a disponibilização dos recursos materiais, tecnológicos e humanos necessários à prestação dos serviços oferecidos aos usuários.

**Art. 13.** Esta Portaria entra em vigor na data de sua publicação.

*(Assinado eletronicamente conf. Lei nº 11.419/2006)*

Desembargador **WELLINGTON JOSÉ DE ARAÚJO**

**Presidente do TRE/AM**