TRIBUNAL REGIONAL ELEITORAL DO PARA

# PORTARIA Nº 18558/2019 TRE/PRE/DG/STI/COINF

Institui a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) no âmbito do Tribunal Regional Eleitoral do Pará.

O DIRETOR DO TRIBUNAL REGIONAL ELEITORAL DO PARÁ, no uso das atribuições que lhe são conferidas por lei,

CONSIDERANDO a RESOLUÇÃO TRE-PA Nº 5.430, DE 27 DE MARÇO DE 2018, que dispõe sobre de diretrizes gerais para a implantação  Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO os Acórdãos 2.746/2010, 7.312/2010, 594/2011 e 866/2011, proferidos pelo Plenário do Tribunal de Contas da União, nos quais foi determinada a instituição de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais;

CONSIDERANDO a importância da adoção de boas práticas relacionadas à proteção da informação preconizadas pelas normas NBR ISO/IEC 27001:2013, NBR ISO/IEC 27002:2013, NBR ISO/IEC 27005:2011;

CONSIDERANDO ainda as disposições insertas nas Normas Complementares n. 05/IN01/DSIC/GSIPR, de 04 de agosto de 2009, e n. 08/IN01/DSIC/GSIPR, de 19 de agosto de 2010, e na Instrução Normativa n. 01 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, que disciplinam a criação e a gestão de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal - APF;

RESOLVE:

Art. 1º Instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), no âmbito do Tribunal Regional Eleitoral do Pará.

Art. 2º Esta Portaria integra a estrutura normativa da Segurança da Informação deste Tribunal, instituída por meio do Art. 8º da Resolução TRE-PA 5.430/2018, de 27 de março de 2018.

## CAPÍTULO I

## DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para os efeitos desta portaria e suas regulamentações, aplicam-se as seguintes definições:

I. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

II. Agente Responsável: servidor público, ocupante de cargo efetivo do TRE-PA, incumbido de chefiar e gerenciar a ETIR;

III. Artefato malicioso: qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas ou redes de computadores;

IV. Comunidade ou público-alvo: conjunto de pessoas, setores, órgãos ou entidades atendidas pela ETIR;

V. Detecção de intrusão: serviço que consiste na análise do tráfego de redes e de histórico de dispositivos que detectam as tentativas de intrusões em redes de computadores, com vistas a identificar e iniciar os procedimentos de resposta a incidentes de segurança em redes computacionais, com base em eventos com características pré-definidas, que possam levar a uma possível intrusão;

VI. Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VII. Serviço: conjunto de procedimentos, estruturados em processo definido, oferecidos à comunidade da ETIR;

VIII. Tratamento de artefatos maliciosos: serviço que consiste em receber informações ou cópia de artefato malicioso que foi utilizado no ataque, ou em qualquer atividade desautorizada ou maliciosa, o qual será analisado, a fim de que seja detectada sua natureza, mecanismo, versão e objetivo, visando ao desenvolvimento de estratégia de detecção, remoção e defesa;

IX. Tratamento de incidentes de segurança em redes computacionais: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas, e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

X. Tratamento de vulnerabilidades: serviço que consiste em receber informações sobre vulnerabilidades, quer sejam em hardware ou software, objetivando analisar sua natureza, mecanismo e suas consequências e desenvolver estratégias para detecção e correção.

## CAPÍTULO II

## DA ESTRUTURA ORGANIZACIONAL

Art. 4º A ETIR será vinculada administrativamente à Secretaria de Tecnologia da Informação deste Tribunal, sendo formada, preferencialmente, por servidores efetivos lotados na Coordenadoria de Infraestrutura e Coordenadoria de Sistemas, os quais, além de suas atividades regulamentares, desempenharão as funções relacionadas ao tratamento e resposta a incidentes em redes computacionais, conforme definido nas portarias que instituem as respectivas unidades.

Art. 5º Os integrantes da equipe serão indicados pelo Secretário de Tecnologia da Informação, e designados por meio de Portaria da Diretoria-Geral.

§ 1º A equipe será composta de igual número de membros titulares e substitutos.

§ 2º A designação do Agente Responsável deverá recair sobre um dos membro titulares.

Art. 6º A ETIR funcionará como um grupo de trabalho permanente, de atuação primordialmente reativa, sem prejuízo de sua responsabilidade quanto a ações preventivas.

§ 1º As atividades reativas da ETIR terão preferência sobre aquelas designadas pelos chefes imediatos de seus respectivos integrantes.

§ 2º As atividades da ETIR poderão ser auxiliadas por colaboradores contratados para esta finalidade, com conhecimento e expertise equivalentes às demandas associadas.

Art. 7º Quando requerida, a ETIR deverá apresentar ao Comitê de Segurança da Informação relatórios estatísticos dos incidentes de segurança ocorridos no período, com os respectivos tratamentos adotados, visando à elaboração de estudos de melhoria dos mecanismos de segurança, ou ainda para fins de subsidiar as decisões estratégicas da Administração, relativamente à segurança da informação.

Parágrafo único. A ETIR deverá efetuar reunião mensal, ou em menor prazo quanto houver necessidade, para planejamento das ações inerentes às suas atividades.

## CAPÍTULO III
## DA AUTONOMIA

Art. 8º A ETIR obedecerá o modelo "Autonomia Completa", o que lhe permitirá conduzir o público-alvo na realização de ações ou medidas necessárias para reforçar a resposta ou a postura da organização, na recuperação de incidentes de segurança, conforme definido pelo fluxo de trabalho pela Secretaria de Tecnologia da Informação.

Parágrafo único. Caso necessário, durante um incidente de segurança, ou em condições emergenciais, a ETIR poderá tomar a decisão de executar as medidas de recuperação, sem aguardar pela aprovação de níveis superiores de gestão.

## CAPÍTULO IV
## DO PÚBLICO-ALVO

Art. 9º A ETIR atenderá, por meio da Central de Serviços de TI, a todos os usuários da rede de computadores e de sistemas do TRE-PA que comunicarem eventos identificados como incidentes de segurança.

Art. 10 A ETIR poderá interagir com unidades de mesma natureza vinculadas a órgãos da Administração Pública Federal, do Poder Legislativo, do Poder Judiciário e do Ministério Público, fornecendo informações acerca dos incidentes de segurança ocorridos na rede de computadores do TRE-PA, com o objetivo de alimentar suas bases de conhecimentos e fomentar a troca de informações sobre incidentes e tecnologias, conforme definido pelo fluxo de trabalho pela Secretaria de Tecnologia da Informação.

Parágrafo único. Nos casos previstos no caput deste artigo, a comunicação dos incidentes de segurança, bem como o tratamento aplicado, será efetuada através de documento formal.

## CAPÍTULO V
## DOS SERVIÇOS E PROCEDIMENTOS

Art. 11. Competirá à ETIR a implementação e o desempenho dos seguintes serviços:

I. tratamento de incidentes de segurança em redes computacionais;

II. tratamento de artefatos maliciosos;

III. tratamento de vulnerabilidades;

IV. monitoramento da segurança da rede de computadores;

V. análise dos processos e procedimentos utilizados;

VI. prospecção ou monitoração de novas tecnologias.

Art. 12. Para cada serviço elencado no artigo anterior deverão ser formalizados os procedimentos a serem observados pela ETIR, por intermédio de documento firmado pelo Agente Responsável, contendo:

I. a definição do serviço;

II. o objetivo do serviço;

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

Parágrafo único. O documento de que trata este artigo deverá ser elaborado pela equipe e submetido ao Comitê de Segurança da Informação, no prazo máximo de 6 (seis) meses após sua nomeação, e atualizado sempre que necessário.

## CAPÍTULO VI
## DAS RESPONSABILIDADES

Art. 13. Caberá ao Agente Responsável:

I. elaborar os procedimentos internos a serem observados pela ETIR, com apoio da própria equipe;

II. gerenciar as atividades desempenhadas pela ETIR;

III. distribuir, sempre que necessário, tarefas para a ETIR, inclusive as de caráter pró-ativo;

IV. sugerir ao Secretário de Tecnologia da Informação e ao Presidente da Comissão de Segurança da Informação, quando necessário, a convocação de representantes de outras unidades da Secretaria, para atuar no tratamento e resposta de determinado incidente de segurança;

V. elaborar documentos técnicos juntamente com a equipe para organizar e tornar mais eficaz desempenho de suas atividades;

VI. assegurar que os usuários estejam informados sobre os procedimentos a serem adotados em relação aos incidentes de segurança da informação.

Art. 14. Caberá à ETIR:

I. formalizar à ETIR/JE os incidentes de segurança em redes computacionais que envolvam ou que possam vir a envolver mais de um Tribunal Eleitoral;

II. atender às orientações da ETIR/JE;

III. manter registro dos incidentes de segurança em redes de computadores notificados ou detectados, com o objetivo de assegurar registro histórico das atividades;

IV. recolher evidências imediatamente após a constatação de um incidente de segurança da informação na rede interna de computadores;

V. executar análise crítica sobre os registros de falha para assegurar que as mesmas foram satisfatoriamente resolvidas;

VI. investigar as causas dos incidentes de segurança da informação na rede interna de computadores;

VII. implementar mecanismos para permitir a quantificação e monitoramento dos tipos, volumes e custos de incidentes e falhas de funcionamento;

VIII. indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências.

IX. auxiliar a Comissão de Segurança da Informação quanto à divulgação de informações referentes à incidentes de segurança e eventos correlatos, objetivando fomentar a cultura de Segurança da Informação no Tribunal.

Art. 15. Caberá ao Secretário de Tecnologia da Informação:

I. submeter ao Diretor-Geral as indicações do Agente Responsável, bem como dos servidores titulares e substitutos que integrarão a ETIR;

II. 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;

III. 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;

**CAPÍTULO VII**

**DAS DISPOSIÇÕES FINAIS**

Art. 16. Os casos omissos serão submetidos à deliberação da Comissão de Segurança da Informação.

Art. 17. Os integrantes da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, bem como o Agente Responsável, deverão ser nomeados no prazo de 30 (trinta) dias úteis, a contar da publicação desta Portaria.

Art. 18. Esta Portaria entra em vigor na data de sua publicação.

OSMAR NELSON ELLERY FROTA

DIRETOR-GERAL

Belém, 02 de abril de 2019.

Documento assinado eletronicamente por **OSMAR NELSON ELLERY FROTA**, **Diretor Geral**, em 03/04/2019, às 15:07, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pa.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0742549** e o código CRC **C0F19709**.

0000585-22.2017.6.14.8000 0742549v6