TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ

Portaria Presidência Nº 526/2022 TRE/PRESI/DG/ASSDG, de 27 de julho de 2022

Estabelece a Política para o Tratamento e Resposta a Incidentes em Redes Computacionais no âmbito do Tribunal Regional Eleitoral do Piauí.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ, no uso de suas atribuições legais e regimentais;

CONSIDERANDO o disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados);

CONSIDERANDO o disposto no inciso VIII do art. 24 da Resolução nº 370, de 28 de janeiro de 2021, do Conselho Nacional de Justiça, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO o disposto na Resolução nº 363, de 12 de janeiro de 2021, do Conselho Nacional de Justiça, que estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos Tribunais;

CONSIDERANDO o disposto na Resolução nº 23.644, de 1º de julho de 2021, do Tribunal Superior Eleitoral, que institui a Política de Segurança da Informação (PSI) da Justiça Eleitoral;

CONSIDERANDO a Política de Segurança da Informação – PSI da Justiça Eleitoral do Piauí, instituída por meio da Resolução nº 448, de 24 de maio de 2022;

CONSIDERANDO o disposto nos Acórdãos nºs 866/2011, 594/2011, 7.312/2010 e 2.746/2010 - Plenário, do Tribunal de Contas da União, que determinaram a instituição de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR;

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 NC 05/IN01/DSIC/GSIPR, de 4 de agosto de 2009, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta;

CONSIDERANDO a NC 08/IN01/DSIC/GSIPR, de 19 de agosto de 2010, que disciplina a gestão da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR, fornecendo diretrizes para o gerenciamento de incidentes em redes computacionais nos órgãos e entidades da Administração Pública Federal;

CONSIDERANDO a Portaria nº 162, de 10 de junho de 2021, do Conselho Nacional de Justiça, que aprova protocolos e manuais criados pela Resolução nº 396, de 7 de junho de 2021, do Conselho Nacional de Justiça, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

RESOLVE:

Art. 1º Fica estabelecida a Política de Tratamento e Resposta a Incidentes em

Redes Computacionais no âmbito do Tribunal Regional Eleitoral do Piauí.

CAPÍTULO I

DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para os efeitos desta Portaria e de suas regulamentações, aplicam-se as seguintes definições:

I - agente responsável: servidora pública ou servidor público, ocupante de cargo efetivo do TRE/PI, incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

II - 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 e/ou redes de computadores;

III - comunidade ou público alvo: conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

IV - crise cibernética: caracteriza-se quando o incidente: apresentar grave dano material ou de imagem; as ações de resposta ao incidente provavelmente persistirão por longo período; gerar impacto na atividade finalística ou serviço crítico mantido pelo Tribunal; ou quando o incidente atrair grande atenção da mídia e da população em geral;

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 - 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;

VII - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VIII - serviço: conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da ETIR;

IX - 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. Uma vez recebido, o mesmo deve ser analisado, ou seja, deve-se buscar a natureza do artefato, seu mecanismo, versão e objetivo, para que seja desenvolvida, ou pelo menos sugerida, uma estratégia de detecção, remoção e defesa;

X - 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;

XI - 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;

XII - vazamento de dados pessoais: acesso e exposição, não autorizada, de informações e dados sigilosos de pessoas físicas ou jurídicas, com objetivo malicioso e criminoso.

CAPÍTULO II

DA MISSÃO

Art. 3º A ETIR do Tribunal Regional Eleitoral do Piauí terá como missão planejar, coordenar e executar atividades de tratamento e resposta a incidentes de segurança da informação, atuando também de forma proativa com o objetivo de minimizar vulnerabilidades e ameaças que possam comprometer o negócio do Tribunal.

CAPÍTULO III

DO PÚBLICO ALVO

Art. 4º A ETIR terá como público alvo todas as pessoas que utilizam os serviços da rede de computadores e de sistemas do TRE/PI, no âmbito da Secretaria do Tribunal e das Zonas Eleitorais e Postos de Atendimento ao Eleitor.

Art. 5º Externamente, poderá a ETIR interagir com outros órgãos da Administração Pública Federal, do Poder Legislativo, do Poder Judiciário e do Ministério Público que atuem no mesmo campo da ETIR, fornecendo informações acerca dos incidentes de segurança ocorridos na rede de computadores do TRE/PI, alimentando as suas bases de conhecimentos e fomentando a troca de tecnologias.

Paragrafo único. A comunicação dos incidentes de segurança, bem como o tratamento aplicado, será efetuada através de documento formal.

CAPÍTULO IV

DO MODELO DE IMPLEMENTAÇÃO

Art. 6º A ETIR será formada preferencialmente por servidoras ou servidores da área de TI, devendo seus membros, além de exercerem suas funções regulares, desempenharem as atividades relacionadas ao tratamento e respostas a incidentes em redes computacionais.

CAPÍTULO V

DA AUTONOMIA

Art. 7º A ETIR seguirá o modelo “Autonomia Compartilhada”, descrito no subitem 9.2 da NC 05/IN01/DSIC/GSIPR, que lhe permitirá trabalhar em acordo com outras unidades do Tribunal a fim de participar do processo de tomada de decisão sobre quais medidas devam ser adotadas.

§ 1º A ETIR participará no resultado da decisão, sendo, no entanto, apenas um membro no processo decisório. Neste caso, a Equipe poderá recomendar os procedimentos a serem executados ou as medidas de recuperação durante um ataque e discutirá as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas) com a unidade a que está hierarquicamente vinculada.

§ 2º Quando a ocorrência de um incidente exigir atuação imediata e emergencial, em função de evento crítico confirmado, relacionado à segurança dos sistemas de computação ou das redes de computadores, a ETIR poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

§ 3º A ETIR também poderá atuar sem esperar pela aprovação de níveis superiores de gestão nos casos em que o incidente registrado seja de simples resolução e não impacte a instituição como um todo.

§ 4º Todos os demais procedimentos ou medidas de recuperação a incidentes em redes computacionais que não se enquadrem no descrito nos parágrafos 2º e 3º deste artigo deverão ser submetidos à aprovação de níveis superiores de gestão.

CAPÍTULO VI

DA ESTRUTURA ORGANIZACIONAL

Art. 8º A ETIR estará vinculada hierarquicamente à Secretaria de Tecnologia da Informação, que constituirá o primeiro nível de gestão superior.

Art. 9º A ETIR será formada, preferencialmente, por servidoras públicas efetivas ou servidores públicos efetivos lotados na área de tecnologia da informação do Tribunal.

§ 1º Para cada integrante titular, será indicado a respectiva substituta ou o respectivo substituto.

§ 2º Seus integrantes, titulares, substitutas ou substitutos, serão indicados pelo titular da Secretaria de Tecnologia da Informação e designados por meio de Portaria da Diretoria-Geral.

§ 3º Dentre os titulares, um deverá ser indicado como Agente Responsável.

§ 4º A ETIR poderá solicitar apoio multidisciplinar para responder os incidentes de segurança de maneira adequada e tempestiva, em áreas como: tecnologia da informação, segurança da informação, jurídica, pesquisas judiciárias, comunicação, controle interno, segurança institucional, entre outras.

Art. 10. 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 de seus respectivos integrantes.

CAPÍTULO VII

DOS SERVIÇOS E PROCEDIMENTOS

Art. 11. São serviços a serem implementados e desempenhados pela ETIR:

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.

Art. 12. Para cada serviço elencado no artigo anterior, 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;

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 atualizado sempre que necessário.

Art. 13. A ETIR deverá apresentar à Comissão de Segurança da Informação relatórios estatísticos dos incidentes de segurança ocorridos em período, a ser definido, com os respectivos tratamentos adotados, com vistas à elaboração de estudos de melhoria dos mecanismos de segurança estabelecidos no Tribunal ou para fins de tomada de decisão estratégica relativa à Segurança da Informação junto à Administração.

CAPÍTULO VIII

DAS RESPONSABILIDADES

Art. 14. 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 proativo;

IV - sugerir à Secretária ou ao Secretário de Tecnologia da Informação, quando necessário, a convocação de representantes de outras unidades da Secretaria de Tecnologia da Informação, para atuar no tratamento e resposta de determinado incidente de segurança;

V - treinar integrantes da equipe, para o fiel desempenho de suas atividades;

VI - assegurar que as pessoas que utilizam os serviços de TI sejam informados sobre os procedimentos adotados em relação aos incidentes de segurança da informação por eles comunicados;

VII - cuidar para a manutenção da capacitação da equipe da ETIR, fazendo constar do Plano Anual de Capacitação os eventos que entender relevantes ao bom desempenho dos trabalhos da equipe.

Art. 15. Caberá à ETIR:

I - manter registro dos incidentes de segurança em redes de computadores notificados ou detectados, com o objetivo de assegurar registro histórico das atividades da ETIR;

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

III - executar análise crítica sobre os registros de falhas para assegurar que estas foram satisfatoriamente resolvidas;

IV - investigar as causas dos incidentes de segurança da informação na rede interna de computadores;

V - implementar mecanismos para permitir a quantificação e monitoração dos tipos, volumes e custos de incidentes e falhas de funcionamento;

VI - indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências de incidentes;

VII - criar um canal de comunicação para os incidentes de segurança da informação para uso com as usuárias ou com os usuários internos e outras ETIRs;

VIII - recomendar os procedimentos a serem executados ou as medidas de recuperação durante a identificação de uma ameaça e discutir as ações a serem tomadas, seus impactos e a repercussão, caso as recomendações não sejam seguidas;

IX - comunicar à STI a ocorrência dos seguintes tipos de incidentes:

a) vazamentos de dados pessoais;

b) os classificados como graves;

c) os definidos como crise cibernética.

Art. 16. Caberá à titular ou ao titular da Secretaria de Tecnologia da Informação:

I - submeter à titular ou ao titular da Diretoria Geral a indicação da Agente Responsável ou do Agente Responsável, das servidoras e dos servidores titulares da ETIR e seus respectivos substitutos;

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 - participar do processo decisório como primeiro nível de gestão superior, decidindo as questões submetidas pela ETIR de acordo com a criticidade e complexidade de cada caso;

IV - notificar à Presidência do TRE-PI os incidentes que impliquem em vazamento de dados pessoais.

Art. 17. Caberá à titular ou ao titular da Diretoria Geral:

I - expedir portaria nomeando a Agente Responsável ou o Agente Responsável, as servidoras e os servidores titulares da ETIR e substitutas e substitutos;

II - participar do processo decisório como segundo nível de gestão superior, decidindo as questões submetidas pela Secretaria de Tecnologia da Informação de acordo com o impacto à continuidade do negócio do Tribunal.

CAPÍTULO IX

DAS DISPOSIÇÕES GERAIS

Art. 18. Os casos omissos e as dúvidas surgidas na aplicação desta Portaria serão dirimidos pela Comissão de Segurança da Informação deste Tribunal.

Art. 19. Este normativo deverá ser revisado periodicamente, em intervalos de, no máximo, dois anos.

Art. 20. Os integrantes da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, titulares e respectivos substitutos, deverão ser designados formalmente, observado o disposto nesta Portaria.

Art. 21. Esta Portaria entra em vigor na data de sua publicação.

Desembargador ERIVAN LOPES

Presidente do TRE/PI

Documento assinado eletronicamente por **Erivan José da Silva Lopes**, **Presidente**, em 28/07/2022, às 10:01, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1595459** e o código CRC **DA1FC39B**.