INSTRUÇÃO NORMATIVA Nº 05/2019.

Regulamenta o funcionamento da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR no âmbito da Justiça Eleitoral do Paraná.

O DIRETOR-GERAL DO TRIBUNAL REGIONAL ELEITORAL, no uso de suas atribuições legais e regimentais,

CONSIDERANDO que esta norma integra a Política de Segurança de Informação da Justiça Eleitoral, estabelecida pela Resolução TSE nº 23.501/2016;

CONSIDERANDO o disposto nos Acórdãos nºs 866/2011, 594/2011, 7312/2010 e 2746/2010 do TCU - Plenário, que determinam a instituição de Equipe 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 ISO NBR/IEC 27001:2013 e 27002:2013;

CONSIDERANDO a NC 05/IN01/DSIC/GSIPR, de 14/08/2009, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, nos órgãos e entidades da Administração Pública Federal, direta e indireta;

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

CONSIDERANDO o contido no PAD nº 8390/2019,

RESOLVE

CAPÍTULO I
DOS CONCEITOS E DEFINIÇÕES

Art. 1º Para os efeitos desta norma aplicam-se as seguintes definições:

I - Agente responsável: servidor público, ocupante de cargo efetivo do TRE-PR, incumbido de gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR;

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 - 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;

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

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

VII - 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; e,

VIII - Vulnerabilidade: é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

CAPÍTULO II
DO OBJETIVO

Art. 2º A ETIR tem como missão principal atuar no tratamento e investigação de incidentes de segurança da informação ocorridos na rede de computadores do TRE-PR.

CAPÍTULO III
DO PÚBLICO ALVO

Art. 3º A ETIR atenderá, prioritariamente, por meio do serviço de registro de chamados na Central de Serviços de TI, a todos os usuários da rede de computadores e de sistemas do TRE-PR que comunicarem eventos identificados como incidentes de segurança.

Parágrafo único. Após a comunicação do incidente, o agente responsável tomará as medidas necessárias, incluindo os registros formais, caso ainda não tenham ocorrido.

Art. 4º 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, fornecendo informações acerca dos incidentes de segurança ocorridos na rede de computadores do TRE-PR, alimentando as suas bases de conhecimentos e fomentando a troca de tecnologias.

CAPÍTULO IV
DO MODELO DE IMPLEMENTAÇÃO

Art. 5º A ETIR será implementada segundo o Modelo 1, da NC 05/IN01/DSIC/GSIPR, sendo formada por servidores efetivos da Secretaria de Tecnologia da Informação que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais.

CAPÍTULO V
DA AUTONOMIA

Art. 6º A ETIR adotará o modelo de "Autonomia Compartilhada", conforme descrito no subitem 9.2 da NC 05/IN01/DSIC/GSIPR, e trabalhará em acordo com os outros setores da organização a fim de participar do processo de decisão sobre quais medidas devem ser adotadas durante o tratamento e recuperação de incidentes de segurança.

Parágrafo único. Durante um incidente de segurança, a ETIR executará as medidas técnicas necessárias para interromper o incidente e preservar as evidências relacionadas, e aguardando pela deliberação de níveis superiores de gestão quanto à recuperação e tratamento do incidente conforme o seu nível de gravidade e impacto.

CAPÍTULO VI
DA ESTRUTURA ORGANIZACIONAL

Art. 7º A ETIR estará vinculada à Secretaria de Tecnologia da Informação.

Art. 8º A ETIR deverá apresentar à Comissão de Segurança da Informação, anualmente, 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 ou para fins de tomada de decisão estratégica relativa à Segurança da Informação.

Art. 9º A ETIR será composta inicialmente pelos titulares das seguintes áreas:

I – Seção de Administração de Banco de Dados;

II – Seção de Administração de Sistemas;

III – Seção de Ambientes de Colaboração;

IV – Seção de Gestão da Central de Serviços;

V – Seção de Infraestrutura de Datacenter e Servidores; e,

VI – Seção de Rede.

§ 1º Para cada integrante titular, o respectivo substituto formalmente designado será seu suplente na ETIR.

§ 2º Dentre os titulares, será inicialmente indicado como Agente Responsável o titular da Seção de Datacenter e Servidores, ficando a cargo do secretário de TI solicitar sua substituição, caso necessário.

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 atividades da ETIR:

I - Tratamento de incidentes de segurança em redes computacionais;

II - Tratamento ou solicitação de tratamento de artefatos maliciosos;

III - Tratamento ou solicitação de tratamento de vulnerabilidades; e,

IV - Análise de processos e procedimentos utilizados pela ETIR.

Art. 12. A formalização dos procedimentos relativos às atividades previstas no art. 11 farão parte do Processo de Tratamento e Resposta a Incidentes em Redes Computacionais, documento a ser elaborado pelo agente responsável e apresentado à CSINF, num prazo não superior a 60 dias da publicação desta instrução normativa.

CAPÍTULO VIII
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 as tarefas para a ETIR, inclusive as de caráter proativo;

IV - Solicitar ao Secretário de Tecnologia da Informação, quando necessário, a convocação de representantes de outras unidades da respectiva secretaria, para atuar no tratamento e resposta de determinado incidente de segurança;

V - Assegurar que os usuários sejam informados sobre os procedimentos adotados em relação aos incidentes de segurança da informação por eles comunicados; e,

VI - Cuidar da capacitação dos membros da ETIR, fazendo constar do Plano Anual de Capacitação os eventos que entender relevantes ao bom desempenho dos trabalhos da equipe.

Art. 14. 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 as mesmas 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; e,

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

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

I - Submeter à Diretoria-Geral a indicação/alteração do agente responsável, dos servidores titulares da ETIR e seus respectivos substitutos; e,

II - Apoiar a ETIR na execução de seu trabalho, viabilizando a disponibilização dos recursos materiais, tecnológicos e humanos necessários às suas atividades.

CAPÍTULO IX
DAS DISPOSIÇÕES GERAIS

Art. 16. Os casos omissos e eventuais dúvidas quanto à aplicação desta norma serão dirimidos pela Comissão de Segurança da Informação deste Tribunal.

Art. 17. Revoga-se a Portaria TRE/PR/DG nº 449/2017.

Art. 18. A ETIR será reinstituída mediante Portaria da Diretoria-Geral.

Art. 19. Esta instrução normativa entra em vigor na data de sua publicação.

Curitiba, 30 de julho de 2019.

VALCIR MOMBACH
Diretor-Geral do TRE/PR