TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE

PRESIDÊNCIA

PORTARIA Nº 423/2017 - GP

Institui a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) no âmbito do TRE/RN.

O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE, no uso das atribuições que lhe são conferidas pelo artigo 20, inciso XIX, da Resolução TRE/RN n.º 09/2012, que aprova o Regimento Interno deste Tribunal;

Considerando a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral, aprovada pela Resolução TSE nº 23501, de 19 de dezembro de 2016;

Considerando o disposto nos Acórdãos TCU nºs. 866/2011, 594/2011, 7312/2010 e 2746/2010 - 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 04.08.2009, 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; e

Considerando a NC 08/IN01/DSIC/GSIPR, de 19.08.2010, que disciplina a gestão da ETIR, fornecendo diretrizes para o gerenciamento de incidentes em redes computacionais nos órgãos e entidades da Administração Pública Federal;

Considerando o que consta do Protocolo PAE nº 8195/2016;

RESOLVE:

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

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: servidor público, ocupante de cargo efetivo do TRE/RN, 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. 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. 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 um processo bem definido, oferecido 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. 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.

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

DO OBJETIVO

Art. 3º A ETIR terá como objetivo garantir o cumprimento da missão institucional do Tribunal Regional Eleitoral do TRE/RN, através do tratamento e resposta a incidentes de segurança na rede interna de computadores.

CAPÍTULO III

DO PÚBLICO ALVO

Art. 4º A ETIR atenderá, por meio do serviço de registro de chamados na Central de Serviços[1], a todos os usuários da rede de computadores e de sistemas do TRE/RN que comunicarem eventos identificados como incidentes de segurança.

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/RN, 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 implementada segundo o Modelo 1, da NC 05/IN01/DSIC/GSIPR, devendo ser formada por servidores efetivos que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais[2].

CAPÍTULO V

DA AUTONOMIA

Art. 7º. A ETIR seguirá o modelo "Autonomia Completa", descrito no subitem 9.1 da NC 05/IN01/DSIC/GSIPR, que lhe permitirá conduzir o seu público alvo na realização de ações ou medidas necessárias para reforçar a resposta ou a postura da organização, na recuperação de incidentes de segurança. Além disso, durante um incidente de segurança, poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão[3].

CAPÍTULO VI

DA ESTRUTURA ORGANIZACIONAL

Art. 8º A ETIR estará vinculada à Secretaria de Tecnologia da Informação deste Tribunal, e terá plena autonomia para desenvolver suas atividades.

---

1 Ou área equivalente.

2 A NC 05/IN01/DSIC/GSIPR propõe, no item 7, 4 modelos de implementação da ETIR que, cuja adoção de modelo específico, segundo a POSIC-JE, será definido pela Comissão de Segurança da Informação do Tribunal.

3 A NC 05/IN01/DSIC/GSIPR propõe, no item 9, outros dois modelos de autonomia da ETIR, que poderão ser adotados, se forem mais coerentes com o nível de responsabilidade que a Equipe tiver sobre suas próprias ações.

Art. 9º Mensalmente, a ETIR deverá apresentar à Comissão de Segurança da Informação 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 no Tribunal ou para fins de tomada de decisão estratégica relativa à Segurança da Informação junto à Administração.

Art. 10. A ETIR será formada, preferencialmente, por servidores públicos efetivos lotados na área de Infraestrutura de Rede de Computadores do Tribunal[4].

§ 1º Para cada integrante titular, será indicado o respectivo substituto.

§ 2º Seus integrantes, titulares e substitutos, serão indicados pelo Secretário de Tecnologia da Informação, e designados por meio de Portaria da DG ou Presidência.

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

Art. 11. 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. 12. 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;

V. análise dos processos e procedimentos utilizados pela ETIR;

VI. prospecção ou monitoração de novas tecnologias.

Art. 13. 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; o

II. o objetivo do serviço; e

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

---

4 A NC 05/IN01/DSIC/GSIPR propõe, no subitem 8.4, recomenda que os membros da ETIR sejam administradores de sistema ou de segurança, administradores de banco de dados, administradores de rede, analistas de suporte ou quaisquer outras pessoas da organização com conhecimento técnico comprovado. Além disso, abre a possibilidade de incluir outras áreas da organização.

Parágrafo único. O documento de que trata este artigo deverá ser elaborado pela Equipe, após sua constituição, no prazo máximo de 180 (cento e oitenta) dias, e atualizados sempre que necessário.

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 pró-ativo;

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

VII. cuidar para a manutenção 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. 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 falha 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. 16. Caberá ao Secretário de Tecnologia da Informação:

I. Submeter ao DG ou Presidente a indicação 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 à prestação dos serviços oferecidos aos usuários.

CAPÍTULO IX
DAS DISPOSIÇÕES GERAIS

Art. 17. Os casos omissos e as dúvidas surgidas na aplicação desta Portaria serão dirimidos pela Presidência deste Tribunal com o subsídio da Comissão de Segurança da Informação deste Tribunal.

Art. 18. Este normativo deverá ser revisado periodicamente, em intervalos de, no máximo, 03 (três) anos.

Art. 19. No prazo de até 10 (dez) dias a contar da publicação desta Portaria, a Comissão de Segurança Permanente de Segurança deverá indicar, nos moldes do art. 26 da Resolução TSE nº 23.501/2016, os nomes dos integrantes da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, titulares e respectivos substitutos.

Art. 20. Esta Portaria entra em vigor na data de sua publicação.

Natal, 28 de novembro de 2017

Desembargador **Dilermando Mota Pereira**
Presidente