Documento de constituição da Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais do Conselho Nacional de Justiça – ETIR - CNJ

1 OBJETIVO

Instituir e regulamentar o funcionamento da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) no Conselho Nacional de Justiça.

2 MISSÃO

Planejar, coordenar e executar atividades de tratamento e resposta a incidentes em redes computacionais, receber e notificar qualquer evento adverso à segurança da informação, confirmado ou sob suspeita, relacionado às redes de computadores, preservando os dados, as informações e a infraestrutura do Conselho Nacional de Justiça.

3 PÚBLICO ALVO

Usuários da rede corporativa de computadores e sistemas do Conselho Nacional de Justiça que registrarem eventos identificados como incidentes de segurança.

4 MODELO DE IMPLEMENTAÇÃO

4.1 A ETIR adotará o modelo de implementação proposto pelo item 7.1 da Norma Complementar nº 05/IN01/DSIC/GSIPR, qual seja, Modelo 1 – Utilizando a equipe de Tecnologia da Informação – TI, e será formada por membros das unidades do Departamento de Tecnologia da Informação (DTI), preferencialmente servidores efetivos, que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais.

4.2 Neste modelo as funções e serviços de tratamento de incidente deverão ser realizadas, preferencialmente, por administradores de rede ou de sistema ou, ainda, por peritos em segurança.

4.3 A Equipe que utilizar este modelo desempenhará suas atividades, via de regra, de forma reativa, sendo desejável, porém, que o Agente Responsável pela ETIR atribua responsabilidades para que os seus membros exerçam atividades pró-ativas.

5 ESTRUTURA ORGANIZACIONAL

5.1 A ETIR será formada por dois integrantes:

5.1.1. Um servidor da Coordenadoria de Infraestrutura e Atendimento (COAI), designado como Agente Responsável.

5.1.2. Um servidor da Seção de Gestão de Segurança da Informação (SEGSI);

5.2 Ao Agente Responsável caberá criar os procedimentos internos, treinar os integrantes, gerenciar as atividades, distribuir tarefas para a equipe, inclusive as de caráter proativo e interfacear a comunicação com o CTIR GOV.

5.3 Seus integrantes serão indicados pelo Diretor do DTI e designados por meio de portaria SG/DG.

5.4 Para cada integrante será indicado e designado o respectivo substituto.

5.5 A ETIR funcionará como um grupo de trabalho permanente, multidisciplinar, de atuação primordialmente reativa e não exclusiva.

5.6 As atividades reativas da ETIR terão prioridade sobre aquelas designadas pelos supervisores de seus respectivos integrantes.

6. AUTONOMIA DA ETIR

A ETIR-CNJ tem autonomia compartilhada, ou seja, participará do resultado da decisão recomendando os procedimentos a serem executados ou as medidas de recuperação durante a identificação de uma ameaça e debaterá as ações a serem tomadas, seus impactos e a repercussão caso as recomendações não forem seguidas.

7. CANAL DE COMUNICAÇÃO

A comunicação dos incidentes de segurança em rede de computadores à ETIR será feita por meio de:

- E-mail: abuse@cnj.jus.br;
- Correspondências oficiais (memorandos, ofícios);
- Pessoalmente, em casos emergenciais;
- Ferramental tecnológico, eventos detectados pelo monitoramento da ETIR.

8. SERVIÇOS

A ETIR prestará os seguintes serviços:

- **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.
- **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.
- **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.

- **Emissão de alertas e advertências:** serviço que consiste em divulgar alertas ou advertências imediatas como uma reação diante de um incidente de segurança em redes de computadores, com o objetivo de advertir a comunidade ou dar orientações sobre como a comunidade deve agir diante do problema.

9. Disposições Gerais

Este documento deverá ser revisado periodicamente, em intervalos de até dois anos.