INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA

PORTARIA Nº 500, DE 13 DE ABRIL DE 2021

O PRESIDENTE DO INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA, no uso das atribuições que lhe foram conferidas pelo art. 19 da Estrutura Regimental, aprovada pelo Decreto nº 10.252, de 20 de fevereiro de 2020, combinado com o art. 110 do Regimento Interno, aprovado pela Portaria nº 531, de 23 de março de 2020, e;

Considerando o disposto no Decreto nº 9.637, de 26 de dezembro de 2018, na Instrução Normativa GSI / PR nº 01, de 13 de junho de 2008; e na Portaria ME / SGD nº 778, de 04 de abril de 2019;

Considerando a necessidade de tratamento e resposta a incidentes de redes computacionais, bem como a obrigação de comunicar às autoridades competentes conforme as melhores práticas e diretrizes do SISP e do GSI/PR, resolve:

Art. 1º Homologar norma complementar à Política de Segurança da Informação e Comunicações do Incra - que institui e dispõe sobre a atuação da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) - com o objetivo de coordenar as atividades de tratamento e resposta a incidentes de segurança ocorridos na Rede desta Autarquia.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

Documento assinado eletronicamente por **Geraldo José da Camara Ferreira de Melo Filho**, **Presidente**, em 15/04/2021, às 19:31, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.incra.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **8628723** e o código CRC **BD27F564**.

ANEXO

NORMA COMPLEMENTAR À POSIC
EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES DE REDES COMPUTACIONAIS (ETIR) DO INCRA

1. CONCEITOS E DEFINIÇÕES

No âmbito desta norma, considera-se:

- Agente Responsável: servidor do Incra, incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

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

- Comunidade ou Público Alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

- CTIR GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações - DSIC do Gabinete de Segurança Institucional da Presidência da República - GSI.

- 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.
- Incidente de Segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.
- Rede: é um sistema de comunicação de dados constituído através da interligação de computadores e outros dispositivos, com a finalidade de trocar informações e partilhar recursos.
- Serviço: é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.
- Tratamento de Incidentes de Segurança em Redes Computacionais: é o 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.
- Usuário: servidores, prestadores de serviço contratados, estagiários, e quaisquer demais agentes públicos ou particulares, vinculados ou não ao Incra, que oficialmente executem atividade relacionada à sua atuação institucional.
- Vulnerabilidade: é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

2. OBJETIVO
2.1 Constituem objetivos da ETIR facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança ocorridos na rede computacional do Incra, por meio de:
a) monitoramento e análise de ataques e intrusões de artefatos maliciosos, identificando possíveis incidentes de segurança;
b) atendimento aos princípios da segurança, integridade e disponibilidade das informações e dos sistemas computacionais disponibilizados pelo Incra;
c) recuperação de informações e sistemas computacionais do Incra;
d) cooperação com outras equipes de tratamento de incidentes dentro e fora da Administração Pública Federal;
e) participação em fóruns e redes nacionais e internacionais, visando à troca de informações; e
f) realização de procedimentos que deverão ser cumpridos por ocasião da coleta e da preservação das evidências.

3. COMUNIDADE OU PÚBLICO ALVO
3.1 A comunidade ou público alvo das atividades da ETIR do Incra são:
a) todos os usuários da rede computacional;
b) demais equipes de resposta a incidentes de segurança da Administração Pública Federal;
c) Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR GOV; e
d) órgãos, entidades e empresas, públicas ou privadas, que tenham contratos ou convênios com o Incra.

4. MODELO DE IMPLEMENTAÇÃO
4.1. A ETIR do Incra será formada por membros da equipe de Tecnologia da Informação que além de suas funções regulares passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais.
4.2 As empresas prestadoras de serviços de TIC poderão ser acionadas para realizar o apoio técnico e suporte necessário as atividades da ETIR.

5. ESTRUTURA ORGANIZACIONAL
5.1. A ETIR do Incra será subordinada à Coordenação Geral de Tecnologia da Informação (DOT).

5.2. O Gestor de Segurança da Informação e Comunicações do Incra será o responsável por prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da ETIR, bem como prover a infraestrutura necessária ao seu funcionamento.

5.3. A ETIR será constituída pelos seguintes membros:
a) Coordenador-Geral de Tecnologia e Gestão da Informação (DOT) que exercerá a função de Agente Responsável;
b) Chefe da Divisão de Desenvolvimento e Manutenção de sistemas (DOT-1);
c) Chefe da Divisão de Infraestrutura de Redes e Comunicação de Dados (DOT-2);
d) Chefe da Divisão de Suporte Técnico (DOT-3).

5.4. Nos impedimentos ou ausências regulares dos membros titulares, os seus substitutos legais exercerão a suplência.

5.5. As atividades relacionadas com administração de redes, de Banco de Dados, de middleware, de mensageria e colaboração, de análise de segurança e de gerência de Engenharia de Software serão exercidas por meio de convocação pelo Agente Responsável da ETIR conforme a necessidade e suportados pelos contratos de prestação de serviços de TIC.

5.6. Os membros realizarão o tratamento e resposta a incidentes em redes computacionais em consonância com suas funções regulares nas respectivas equipes de Tecnologia da Informação e Comunicação.

6. AUTONOMIA
6.1. A autonomia da ETIR do Incra será completa nos casos justificados de incidentes de segurança, podendo a Equipe executar as medidas de recuperação, sem a necessidade de esperar pela aprovação de níveis superiores de gestão.

6.2. A autonomia da ETIR será compartilhada quando ela trabalhar em comum acordo com os outros setores do Incra a fim de participar do processo de tomada de decisão sobre quais medidas devam ser adotadas.

6.3. A ETIR participará do resultado da decisão, na qualidade de membro do processo decisório.
6.3.1. 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.

6.4. A ETIR não fará a apuração ou investigação dos incidentes (análise forense), mas deverá comunicar a ocorrência de incidentes de segurança em redes de computadores ao Centro de Tratamento e Resposta a Incidentes - CTIR GOV, conforme procedimentos a serem definidos pelo próprio CTIR GOV, com vistas a permitir soluções integradas para a Administração Pública Federal - APF, bem como a geração de estatísticas.
6.4.1. Após a comunicação, nos casos aplicáveis, a autoridade responsável pelo Incra deverá, de imediato, encaminhá-la formalmente à autoridade com atribuição de apurar os fatos.

7. SERVIÇOS
7.1. O serviço de tratamento de incidentes de redes visa manter os sistemas e a estrutura de segurança confiável. Consiste em receber, filtrar, classificar e responder solicitações e alertas, identificando tendências de ataques e vulnerabilidades.
7.1.1. As atividades de tratamento e resposta a incidentes serão realizadas sempre que uma solicitação for recebida ou quando ameaças à Rede de Serviços do Incra forem identificadas.
7.1.1.1. As solicitações serão recebidas por meio do Canal de Atendimento da Central de Serviços de Tecnologia da Informação ou diretamente pelo Agente Responsável (DOT), e submetidas à ETIR.

7.2. Os incidentes notificados ou detectados que tenham materialidade ou evidências devem ser registrados em processo SEI específico com classificação Sigilosa, com a finalidade de assegurar registro histórico das atividades da ETIR.

8. DISPOSIÇÕES FINAIS

8.1. Os casos omissos e as dúvidas com relação a esta Norma serão submetidos ao Comitê de Segurança da Informação e Comunicações - CSIC.

8.2. Esta Norma Complementar entra em vigor a partir da data da sua publicação e ficam revogadas todas as disposições em contrário.

REFERÊNCIAS NORMATIVAS:

- Instrução Normativa GSI-PR n. 01 de 13 de junho de 2008, que disciplina a gestão de segurança da informação e comunicações na administração Pública Federal, direta e indireta, e dá outras providências. Gabinete de Segurança Institucional - Presidência da República.

- Norma Complementar nº 05/IN01/DSIC/GSIPR - 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 - APF.

- Norma Complementar nº 08/IN01/DSIC/GSIPR - que dispõe sobre gerenciamento de incidentes de redes computacionais nos órgãos e entidades da Administração Pública Federal - APF.

- Lei n° 12.737, de 30 de novembro de 2012, dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

- Portaria nº 500, de 13 de abril de 2021, aprova a Política de Segurança da Informação e Comunicações - PoSIC do Incra.

- Portaria nº 825, de 28 de abril de 2020, institui o Comitê de Segurança da Informação e Comunicações - CSIC no Incra (6087785) - alterada pela Portaria nº 2181, de 14 de dezembro de 2020 (7816403).