



**MINISTÉRIO DA INDÚSTRIA, COMÉRCIO EXTERIOR E SERVIÇOS  
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL  
PRESIDÊNCIA**

**RESOLUÇÃO Nº 168, DE 21 DE JUNHO DE 2016**

**Assunto:** Aprova a instituição e o funcionamento da equipe de tratamento e resposta à incidentes em redes computacionais do INPI - ETIR-INPI.

**O PRESIDENTE do INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL**, no uso da atribuição que lhe confere o Artigo 23, Inciso XI, do Anexo I, do Decreto nº 8.686, de 04 de março de 2016 e o **COORDENADOR-GERAL DE TECNOLOGIA DA INFORMAÇÃO**,

**CONSIDERANDO** o Decreto nº 3.505, de 13 de junho de 2000, que instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

**CONSIDERANDO** a Instrução Normativa nº 01, de 13 de junho de 2008, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal;

**CONSIDERANDO** a Norma Complementar nº 05, de 14 de agosto de 2009, do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, que disciplina a criação de Equipe de Tratamento e Resposta à Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal;

**CONSIDERANDO** a Norma Complementar nº 08, de 19 de agosto de 2010, do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, que Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.

**CONSIDERANDO** a Instrução Normativa nº 24, de 29 de julho de 2013, do Instituto Nacional da Propriedade Industrial, que institui a Política de Segurança da Informação e Comunicações – POSIC, no âmbito do INPI;

**CONSIDERANDO** as deliberações constantes da 1ª reunião, Ata Nº 001/2015 PR/INPI, de 28 de outubro de 2015, do Comitê de Segurança da Informação e Comunicações - CSIC, do Instituto Nacional da Propriedade Industrial, que institui a Política de Segurança da Informação e Comunicações – POSIC;

## RESOLVEM:

Art. 1º Instituir a Equipe de Tratamento e Resposta à Incidentes em Redes Computacionais do Instituto Nacional da Propriedade Industrial – ETIR-INPI, subordinada à Coordenação de Infraestrutura, Suporte e Segurança da Informação, observando as diretrizes estabelecidas na Política de Segurança da Informação e Comunicações - POSIC do INPI.

Art. 2º Para efeitos desta Norma, são estabelecidos os seguintes conceitos e definições:

I. **Agente responsável:** Servidor Público ocupante de cargo efetivo do INPI incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta à Incidentes em Redes Computacionais;

II. **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 o funcionamento de sistemas e/ou redes de computadores;

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

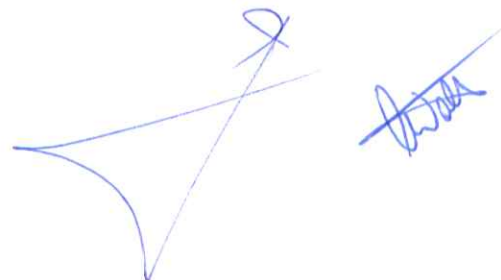
IV. **CTIR GOV:** Centro de Tratamento e Resposta à Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI;

V. **Equipe de Tratamento e Resposta à Incidentes em Redes Computacionais – ETIR:** Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas à incidentes de segurança em redes de computadores;

VI. **Incidente de segurança:** é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VII. **Serviço:** é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta à Incidentes em Redes Computacionais;

VIII. **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;



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

Art. 3º A equipe de resposta à Incidentes de Segurança em Redes Computacionais do INPI, ETIR-INPI, tem como missão facilitar e coordenar as atividades de tratamento e resposta à incidentes em redes computacionais, atuando também de forma proativa com o objetivo de minimizar vulnerabilidades e ameaças que possam comprometer o Instituto.

Art. 4º O público alvo das atividades pertinentes à ETIR-INPI incluem:

I. Todos os servidores e colaboradores que exercem suas atividades no âmbito do INPI;

II. Demais equipes de resposta à incidentes de segurança da informação e comunicações da Administração Pública Federal;

III. Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR GOV;

IV. Órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos ou convênios com o INPI para o intercâmbio de informações;

V. Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República.

Art. 5º A ETIR-INPI adota o Modelo 4 – combinado ou misto, descrito na Norma Complementar nº 05/IN01/DSIC/GSIPR, para o qual será utilizada uma Equipe Central de tratamento e respostas à incidentes e equipes de apoio distribuídas pela organização.

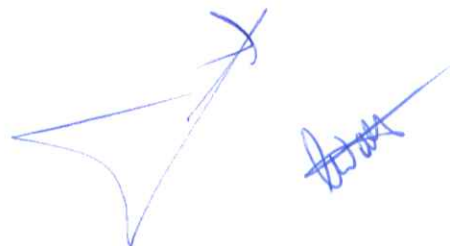
§ 1º A Equipe Central será a responsável por criar as estratégias, gerenciar as atividades e distribuir as tarefas entre as Equipes Distribuídas, além de ser a responsável, perante toda a organização, pela comunicação com o CTIR GOV.

§ 2º As Equipes Distribuídas serão responsáveis por implementar as estratégias e exercer suas atividades em suas respectivas áreas de responsabilidade.

Art. 6º A ETIR-INPI ficará subordinada à Coordenação de Infraestrutura, Suporte e Segurança da Informação – COINF, da Coordenação Geral de Tecnologia da Informação – CGTI.

§ 1º O Agente Responsável pela ETIR-INPI será o coordenador da Coordenação de Infraestrutura, Suporte e Segurança da Informação – COINF.

§ 2º A Equipe Central será formada pelos servidores públicos da Divisão de Segurança da Informação e Gestão de Riscos – DISEG, sendo substituídos, em casos



fortuitos, por servidores públicos do Serviço de Atendimento ao Usuário e Administração de Redes – SERED.

§ 3º As Equipes Distribuídas serão formadas por servidores da Coordenação-Geral de Tecnologia da Informação - CGTI com o conhecimento e o perfil necessário para atuação nas respectivas áreas de responsabilidade: sistemas de informação; banco de dados; infraestrutura e suporte de TIC.

§ 4º A investigação da causa raiz de incidentes de segurança em redes computacionais, bem como a contenção e erradicação são coordenadas pela Equipe Central, e esta deverá ser subsidiada pela equipe distribuída, independente da subordinação ou hierarquia, objetivando clareza, inviolabilidade e veracidade para registro.

§ 5º A ETIR-INPI poderá ser estendida com o apoio consultivo de representantes legais de áreas específicas do Instituto, advogados, estatísticos, recursos humanos, controle interno, consultores técnicos, grupo de investigação ou qualquer outro que a equipe entenda ser adequado para o desenvolvimento de suas atividades.

§ 6º A omissão, subtração, destruição, desfiguração, ocultação, modificação de informações ou a não preservação de evidências de incidentes que impeçam a execução das atividades da ETIR-INPI serão informadas ao Comitê de Segurança da Informação e Comunicações - CSIC, para as providências cabíveis.

Art. 7º Ao agente responsável da ETIR-INPI compete:

I. Coordenar a instituição, implementação e manutenção da infraestrutura necessária a ETIR-INPI;

II. Coordenar e orientar os membros da ETIR-INPI na gestão de incidentes em redes computacionais;

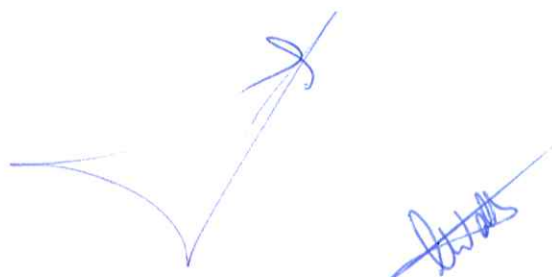
III. Gerenciar as atividades, os procedimentos internos e distribuir as tarefas para os integrantes da ETIR-INPI;

IV. Coordenar o processo de capacitação e treinamento dos membros da ETIR-INPI.

V. Representar a ETIR-INPI como membro nos processos decisórios do Comitê de Segurança da Informação e Comunicações – CSIC, recomendando os procedimentos a serem executados ou as medidas de recuperação durante um ataque e discutir as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas).

Parágrafo único. O exercício do encargo de que trata o caput dar-se-á sem prejuízo de suas atribuições típicas do cargo.

Art. 8º À Equipe Central da ETIR-INPI compete:



I. Registrar, analisar, investigar e tratar incidentes de segurança em redes computacionais;

II. Emitir relatórios de notificações sobre novas ameaças e atualizações de softwares;

III. Recomendar controles aperfeiçoados ou adicionais para limitar a frequência, os danos e os impactos de futuras ocorrências de incidentes em rede computacionais.

IV. Estabelecer canais de comunicação com atores externos tais como Centro de Tratamento de Incidentes de Segurança de Redes de Computadores - CTIR Gov - da Administração Pública Federal - APF, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT Br, Centro de Atendimento a Incidentes de Segurança - CAIS - da Rede Nacional de Ensino e Pesquisa - RNP, Autoridades Legais (Ministério Público, Polícia Federal, entre outros), outras ETIRs de órgãos da APF.

Art. 9º Às Equipes Distribuídas da ETIR-INPI compete:

I. Analisar, investigar e auxiliar no tratamento de incidentes de segurança em suas respectivas áreas de responsabilidade;

II. Executar procedimentos de contenção, tratamento e erradicação de incidentes de segurança em suas respectivas áreas de responsabilidade;

III. Identificar e reportar à Equipe Central a causa raiz de incidentes de segurança em suas respectivas áreas de responsabilidade;

IV. Recomendar controles aperfeiçoados ou adicionais para limitar a frequência, os danos e os impactos de futuras ocorrências de incidentes de segurança em suas respectivas áreas de responsabilidade.

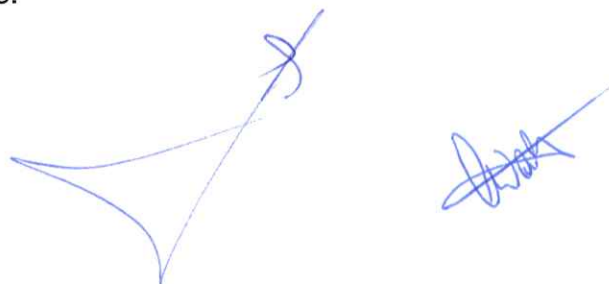
Art. 10º Ao Comitê de Segurança da Informação e Comunicações - CSIC compete:

I. Revisar e aprovar estratégias de tratamento e resposta à incidentes propostos pela ETIR-INPI;

II. Definir acessos à internet e recursos condizentes a participação da Equipe Central da ETIR-INPI na elucidação de incidentes;

III. Aprovar a constituição, alterações na estrutura e a autonomia da ETIR-INPI.

Art. 11 A autonomia da ETIR-INPI é fundamentada nas recomendações da Norma Complementar nº 05 do DSIC/GSI/PR, sendo definida como compartilhada, tendo suas decisões submetidas ao Gestor de Segurança da Informação e Comunicações, ao Comitê de Segurança da Informação e Comunicações - CSIC e ao Coordenador da Coordenação de Sistemas de Informação e Administração de Dados.



§ 1º A ETIR-INPI participará, através do seu agente responsável, no resultado da decisão, sendo, no entanto, apenas um membro no processo decisório.

§ 2º Uma vez tomada a decisão, a ETIR-INPI tem plenas condições e autonomia de adotar as medidas necessárias para a recuperação e tratamento do incidente de segurança.

§ 3º Durante um incidente de segurança em redes de computadores, se houver comprovado prejuízo à imagem institucional ou ameaça efetiva que resulte no comprometimento da segurança das informações e comunicações, a ETIR-INPI poderá tomar a decisão de executar as medidas necessárias para conter/erradicar o incidente, sem esperar pelo processo de tomada de decisão. Tão logo sejam disparadas as ações emergenciais, as instâncias superiores deverão ser informadas.

Art. 12 A ETIR-INPI proverá, a partir de sua instituição, os seguintes serviços:

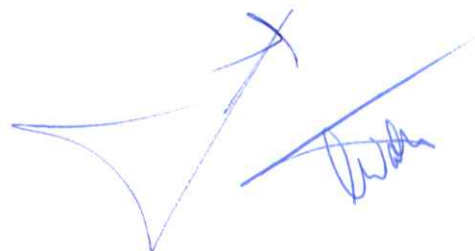
I. Tratamento e resposta de incidentes de segurança em redes computacionais - Este serviço prevê receber, analisar e responder às notificações e atividades relacionadas à incidentes de segurança em redes de computadores. Será prestado durante o horário de expediente normal do órgão, recebendo as notificações e solicitações através do e-mail [abuse@inpi.gov.br](mailto:abuse@inpi.gov.br);

II. Tratamento de artefatos maliciosos - Este serviço prevê o recebimento de informações ou cópia do artefato malicioso que foi utilizado no ataque ou em qualquer outra atividade maliciosa. Será prestado durante o horário de expediente normal do órgão, recebendo as notificações e solicitações através do e-mail [abuse@inpi.gov.br](mailto:abuse@inpi.gov.br);

III. Tratamento de vulnerabilidades - Este serviço prevê o recebimento de informações sobre vulnerabilidades, quer sejam em *hardware* ou *software*, objetivando analisar sua natureza, mecanismo e suas consequências e desenvolver estratégias para detecção e correção dessas vulnerabilidades. Será prestado durante o horário de expediente normal do órgão, recebendo as notificações e solicitações através do e-mail [abuse@inpi.gov.br](mailto:abuse@inpi.gov.br);

IV. Detecção de intrusão - Este serviço prevê a análise do histórico de dispositivos que detectam as tentativas de intrusões em redes de computadores, com vistas a identificar e iniciar os procedimentos de resposta à incidente de segurança em redes de computadores, com base em eventos com características pré-definidas, que possam levar a uma possível intrusão e, ainda, possibilitar o envio de alerta em consonância com padrão de comunicação previamente definido entre a ETIR-INPI e o CTIRGov;

V. Anúncios - Este serviço consiste em divulgar, de forma proativa, alertas sobre vulnerabilidades e problemas de incidentes de segurança em redes de computadores em geral, cujos impactos sejam de médio e longo prazo, possibilitando que a comunidade se prepare contra novas ameaças. Será prestado durante o horário de expediente, conforme



necessidade, mas sem periodicidade definida e sempre através dos mecanismos formais de comunicação da Coordenação-Geral de Comunicação Social – CGCOM;

VI. Emissão de alertas e advertências - Este serviço consiste em divulgar alertas ou advertências imediatas como uma reação diante de um incidente de segurança em redes de computadores ocorrido, com o objetivo de advertir a comunidade ou dar orientações sobre como a comunidade deve agir diante do problema. Será prestado durante o horário de expediente, conforme necessidade, mas sem periodicidade definida e sempre através dos mecanismos formais de comunicação da Coordenação-Geral de Comunicação Social – CGCOM;

VII. Prospecção ou monitoração de novas tecnologias - Este serviço prospecta e/ou monitora o uso de novas técnicas das atividades de intrusão e tendências relacionadas, as quais ajudarão a identificar futuras ameaças. Este serviço inclui a participação em listas de discussão sobre incidentes de segurança em redes de computadores e o acompanhamento de notícias na mídia em geral sobre o tema;

VIII. Avaliação de segurança - Este serviço consiste em efetuar uma análise detalhada da infraestrutura de segurança em redes de computadores e de sistemas de informação do INPI, com base em requisitos da própria organização ou em melhores práticas de mercado.

Art. 13 Dúvidas e casos omissos serão resolvidos pelo Comitê de Segurança da Informação e Comunicações - CSIC;

Art. 14 Esta Resolução entra em vigor na data de sua publicação no Boletim de Pessoal.



**Luiz Otávio Pimentel**  
Presidente



**Eduardo Wallier Vianna**  
Coordenador-Geral de Tecnologia da Informação