**INSTITUTO DE PESQUISA ECONÔMICA APLICADA**

PORTARIA Nº 139 , DE 10 DE MAIO DE DE 2011.

Aprova a instituição e o funcionamento da equipe de tratamento e resposta a incidentes em redes computacionais do IPEA.

O **COMITÊ DE TECNOLOGIA DA INFORMAÇÃO DO INSTITUTO DE PESQUISA ECONÔMICA APLICADA - IPEA**, com fundamento no inciso IV do art. 3º da Portaria Nº 321, de 21 julho de 2010, e

Considerando a) manter a segurança da informação e comunicações de uma organização em um ambiente computacional mundialmente interconectado como grande desafio e que a estratégia de segurança da informação é implementada por meio de várias iniciativas, sendo uma delas a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR;

Considerando b) a portaria nº 456, de 2 de dezembro de 2010, que institui a Política de Segurança da Informação e Comunicações – POSIC, no âmbito do IPEA;

Considerando c) a Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República, de 13.06.2008, que disciplina a gestão de segurança da informação e comunicações no âmbito da Administração Pública Federal;

Considerando d) a Norma Complementar Nº 05 à Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República, 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 – APF;

Considerando e) a Norma Complementar Nº 08 à Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República, de 19.08.2010, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;

**Resolve:**

Art. 1º Fica aprovada na forma desta resolução a instituição e o funcionamento da equipe de tratamento e resposta a incidentes em redes computacionais do Ipea, em complemento à diretriz estabelecida pelo inciso II do art. 7º da Política de Segurança da Informação e Comunicações - POSIC do IPEA, conforme definido a seguir.

## CAPÍTULO I – DA ABRANGÊNCIA E CAMPO DE APLICAÇÃO

Art. 2º A equipe de resposta a Incidentes de Segurança em Redes Computacionais do IPEA, ETIR-IPEA, tem por missão receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança da informação e comunicações em sistemas computacionais no âmbito do IPEA, atuando também de forma proativa com o objetivo de minimizar vulnerabilidades e ameaças que possam comprometer o negócio da Instituição.

Art. 3º O público alvo das atividades pertinentes à ETIR-IPEA incluem:

I - Todos os servidores e colaboradores que exercem suas atividades no âmbito do IPEA;

II - Demais equipes de resposta a 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 IPEA para o intercâmbio de informações;

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

## CAPÍTULO II – DOS TERMOS E DEFINIÇÕES

Art. 4º - Para efeitos desta resolução, ficam estabelecidos os seguintes termos e definições, em complemento daqueles definidos na POSIC do IPEA:

I - Agente Responsável: Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a 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 a Incidentes em Redes Computacionais;

IV - 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;

V - 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;

VI - Incidente de Segurança da Informação: um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

VII - 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;

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;

## CAPÍTULO II – DO MODELO DE IMPLANTAÇÃO E FUNCIONAMENTO

Art. 5º A ETIR-IPEA seguirá o modelo de implantação utilizando a equipe de Tecnologia da Informação do IPEA, de acordo com a definição da Norma Complementar Nº 05 à Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República, de 04.08.2009, conforme definido a seguir:

I - A equipe é composta por profissionais da área de Tecnologia da Informação lotados na sede do IPEA e em suas unidades descentralizadas, sem prejuízo de suas atribuições típicas do cargo, com experiência e conhecimentos técnicos compatíveis com a importância da missão da ETIR-IPEA;

II - A equipe será composta preferencialmente por servidores públicos de carreira, salvo casos atípicos.

III - A ETIR-IPEA ficará vinculada à Coordenação Geral de Tecnologia da Informação e Comunicações - CGTIC, da Diretoria de Desenvolvimento Institucional - DIDES do IPEA

IV - A equipe será chefiada pelo Agente Responsável, designado pelo Coordenador Geral de Tecnologia da Informação e Comunicações do IPEA.

V - Toda a comunicação com organismos externos de resposta a incidentes, especialmente o CTIR.GOV, é responsabilidade do Agente Responsável;

Art. 6º A ETIR-IPEA possui autonomia compartilhada com o Gestor de Segurança da Informação a fim de participar do processo de tomada de decisão sobre quais medidas devam ser adotadas.

§ 1º As decisões serão tomadas pelo Gestor de Segurança da Informação e, na sua ausência, pelo Coordenador Geral de Tecnologia da Informação e Comunicações do IPEA;

§ 2º A ETIR-IPEA participará no resultado da decisão, recomendando os procedimentos, medidas e ações a serem executados para o tratamento e a recuperação durante um incidente, bem como indicando as repercussões se as recomendações não forem seguidas;

§ 3º Durante um incidente de segurança, se tal se justificar, a Equipe poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

§ 4º Uma vez tomada a decisão, a ETIR-IPEA tem plenas condições e autonomia de adotar todas as medidas necessárias para a recuperação e tratamento do incidente;

Art. 7º. A ETIR-IPEA deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede orientados pelo Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV.

Art. 8º. A ETIR-IPEA poderá usar as melhores práticas de mercado, desde que não conflitem com os dispositivos da legislação em vigor;

Art. 9º. A ETIR deverá comunicar de imediato a ocorrência de todos os incidentes de segurança ocorridos na sua área de atuação ao CTIR GOV, conforme padrão definido por aquele órgão, a fim de permitir a geração de estatísticas e soluções integradas para a Administração Pública Federal.

## CAPÍTULO III – DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 10º. Compete ao Gestor de Segurança da Informação e Comunicações:

I - Coordenar a instituição, implementação e manutenção da infraestrutura necessária às Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais, no IPEA, conforme descrito no inciso V do art 5º da Instrução Normativa nº 01, do Gabinete de Segurança Institucional, de 13 de junho de 2008;

II - Durante o gerenciamento de incidentes de segurança em redes de computadores, havendo indícios de ilícitos criminais, o Gestor de Segurança da Informação e Comunicações do IPEA têm como dever, sem prejuízo do disposto no item 6 da Norma Complementar nº 08/IN01/DSIC/GSIPR e do item 10.6 da Norma Complementar nº 05/IN01/DSIC/GSIPR:

a) Acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários;

b) Observar os procedimentos para preservação das evidências exigindo consulta às orientações sobre cadeia de custódia, conforme ato normativo específico a ser expedido;

c) Priorizar a continuidade dos serviços da ETIR e da missão institucional do IPEA, observando os procedimentos previstos no inciso acima.

Art. 11º. Compete à ETIR-IPEA:

I - Prover na sede do IPEA em Brasília e em suas unidades descentralizadas os serviços definidos no Capítulo IV desta resolução, em horário comercial, isto é, das 08:00 até as 18:00hs, de segunda a sexta-feira.

II - Definir e documentar metodologia e procedimentos internos para o tratamento e resposta a incidentes.

III - Criar as estratégias de resposta a incidentes de rede, elaborar procedimentos de resposta para incidentes previamente conhecidos, gerenciar e atribuir as atividades para a equipe distribuída;

IV - Auxiliar o Gestor de Segurança da Informação e Comunicações na tomada de decisões;

Parágrafo único. Na ocorrência de incidentes, a ETIR poderá ser acionada fora do horário comercial, inclusive finais de semana e feriados, como forma de analisar e prover resposta aos mesmos;

Art. 12º. Compete ao Coordenador Geral de Tecnologia da Informação e Comunicações do IPEA:

I - Designar entre os membros de sua equipe os profissionais que farão parte da ETIR-IPEA;

II - Designar entre os membros de sua equipe o Agente Responsável pela ETIR-IPEA;

Art. 13º Compete ao Agente responsável pela ETIR-IPEA:

I - Coordenar as atividades da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

II - Interagir com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV;

III - Criar os procedimentos internos, gerenciar as atividades e distribuir tarefas para a Equipe que compõe a ETIR-IPEA.

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

## CAPÍTULO IV – DOS SERVIÇOS E PROCEDIMENTOS

Art. 14º. A ETIR-IPEA deve prover, no mínimo, o serviço de Tratamento de Incidentes de Redes Computacionais.

Parágrafo único. Este serviço tem por objetivo manter os sistemas e a estrutura de segurança o mais confiável possível. Faz parte deste serviço os procedimentos de receber, filtrar, classificar e responder solicitações e alertas, analisando essas informações a fim de identificar tendências de ataques.

Art. 15º. A ETIR-IPEA deverá oferecer os seguintes serviços complementares, conforme definido na Norma Complementar nº 08/IN01/DSIC/GSIPR, observadas as necessidades e limitações institucionais e de forma gradativa, de acordo com a maturidade da equipe:

I - 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;

II - 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 computado-

res ocorrido, com o objetivo de advertir a comunidade ou dar orientações sobre como a comunidade deve agir diante do problema;

III - 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;

IV - 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;

V - Avaliação de segurança - Este serviço consiste em efetuar uma análise detalhada da infraestrutura de segurança em redes de computadores e de sistemas de informação da organização com base em requisitos da própria organização ou em melhores práticas de mercado. O serviço pode incluir: revisão da infraestrutura, revisão de processos, análise de aplicativos, avaliação de sistemas de informação, varredura da rede e testes de penetração;

VI - 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 a 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-IPEA e o CTIR Gov.

VII - Disseminação de informações relacionadas à segurança - Este serviço fornece de maneira fácil e abrangente a possibilidade de encontrar informações úteis no auxílio do tratamento de incidentes de segurança em redes computacionais.

Parágrafo único. Os serviços disponíveis devem ser divulgados pelo Gestor de Segurança da Informação e Comunicações.

Art. 16º. A ETIR-IPEA deve observar e adotar, no mínimo, os seguintes aspectos e procedimentos:

I - Registro de incidentes de segurança em redes de computadores: todos os incidentes notificados ou detectados devem ser registrados, com a finalidade de assegurar registro histórico das atividades da ETIR;

II - Tratamento da informação: o tratamento da informação pela ETIR deve ser realizado de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo;

III - Recursos disponíveis: a ETIR deve possuir os recursos materiais, tecnológicos e humanos, suficientes para prestar os serviços oferecidos para sua comunidade;

IV - Capacitação dos membros da ETIR: os membros da ETIR devem estar capacitados para operar os recursos disponíveis para a condução dos serviços oferecidos para a sua comunidade;

## CAPÍTULO V – DAS DISPOSIÇÕES FINAIS

Art. 17º. Assuntos de interesse relevantes serão levados ao Comitê de Tecnologia da Informação e Comunicações visando, principalmente, a prevenção de novos incidentes de segurança.

Art. 18º. Casos omissos serão resolvidos pelo Gestor de Segurança da Informação e Comunicações do IPEA, observando-se a legislação em vigor.

Art. 19º. Esta Portaria entra em vigor na data de sua publicação.

**MARCIO POCHMANN**

**Presidente do IPEA**