ANEXO

Instituição da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) no Ministério da Ciência, Tecnologia e Inovação (MCTI).

1 REFERÊNCIA NORMATIVA

1.1 Instrução Normativa nº 1, de 13 de junho de 2008, do Gabinete de Segurança Institucional da Presidência da República, doravante denominada IN01/DSIC/GSIPR: disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta.
1.2 Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, doravante denominada NC05: trata da Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais no âmbito da Administração Pública Federal.
1.3 Política de Segurança da Informação e Comunicações (POSIC) do MCTI, aprovada por meio da Portaria nº 853, de 5 de setembro de 2013, publicada no Diário Oficial da União em 06 de setembro de 2013.

2 DEFINIÇÕES

Além dos conceitos e definições estabelecidos nos documentos que compõem a referência normativa, ficam estabelecidos os seguintes:

2.1 Detecção de Intrusão: é o serviço que consiste na análise do histórico de dispositivos que detectam as tentativas de intrusões em redes de computadores, com vistas a identificar e iniciar, mediante autorização, 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 e, ainda, possibilitar envio de alerta em consonância com o padrão de comunicação previamente definido entre a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR (MCTI) e o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal – CTIR GOV.
2.2 Tratamento de Vulnerabilidades: é o serviço que consiste em receber informações sobre vulnerabilidades, quer sejam em *hardware* ou *software*, objetivando analisar sua natureza, seu mecanismo e suas consequências e desenvolver estratégias para detecção e correção.
2.3 Supervisor: chefe imediato.

3 MISSÃO

É missão da ETIR coordenar e executar as atividades de tratamento e resposta a incidentes em redes computacionais no ambiente do MCTI, tendo como objetivos básicos: monitorar as redes computacionais, detectar e analisar ataques e intrusões, tratar incidentes, vulnerabilidades e artefatos maliciosos, recuperar sistemas, prover e incentivar a cooperação com outras equipes, bem como participar de fóruns e redes nacionais e internacionais.

4 COMUNIDADE OU PÚBLICO ALVO

4.1 A ETIR atenderá a todos os usuários de serviços computacionais dos órgãos de assistência direta e imediata ao Ministro de Estado, dos órgãos específicos e singulares e das unidades descentralizadas do MCTI, preferencialmente por chamado registrado eletronicamente, por meio da Central de Serviços – MCTI.
4.2 A ETIR se relacionará com o CTIR Gov (Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal – APF), por meio de *email* ou telefone a ser devidamente cadastrado. Assim, ataques percebidos pelo CTIR Gov poderão ser informados ao ETIR do MCTI, bem como ajuda poderá ser solicitada àquele CTIR Gov em caso de ataques cuja gravidade assim o exija.

5 MODELO DE IMPLEMENTAÇÃO

5.1 A ETIR será estabelecida segundo o Modelo 1 da NC05/2009 e será formada por membros da Coordenação-Geral de Gestão da Tecnologia da Informação do Ministério da Ciência, Tecnologia e Inovação – CGTI/MCTI, preferencialmente servidores efetivos, que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais.

6 ESTRUTURA ORGANIZACIONAL

6.1 A ETIR será formada por quatro integrantes:

6.1.1 Três servidores da Coordenação de Gerência de Rede, um deles designado Agente Responsável;

6.1.2 Um servidor da Coordenação de Desenvolvimento de Sistemas.

6.2 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.

6.3 Seus integrantes serão indicados pelo Coordenador-Geral da Coordenação-Geral de Gestão da Tecnologia da Informação (CGTI/MCTI) e designados por meio de portaria do Comitê de Segurança de Informações e Comunicações (CSIC).

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

6.5 A indicação dos integrantes, assim como a dos respectivos substitutos, levará em conta a necessidade de ao menos dois integrantes da equipe estarem disponíveis durante todo o horário de expediente do MCTI, sendo um deles no papel de Agente Responsável.

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

6.7 As atividades reativas da ETIR terão prioridade sobre as proativas que venham a ser designadas pelos supervisores de seus respectivos integrantes.

6.8 Cada integrante poderá dedicar até 45 (quarenta e cinco) minutos diários em tarefas proativas, caso estas sejam atribuídas pelo Agente Responsável.

6.9 Extraordinariamente, o Agente Responsável poderá convocar representantes de outras unidades da CGTI/MCTI para atuar em tratamento e resposta de determinado incidente de segurança.

7 AUTONOMIA DA ETIR

7.1 A ETIR seguirá o modelo "Sem Autonomia" da NC05/2009, em que só poderá agir com autorização do Coordenador-Geral da CGTI ou de um de seus Coordenadores.

7.2 Após acionada, caberá à ETIR recomendar procedimentos a serem executados ou as medidas de recuperação a serem adotadas.

7.3 Uma vez acatadas as recomendações e medidas, a ETIR poderá conduzir os tomadores de decisão a agir durante um incidente de segurança.

7.4 Quando conveniente e necessário, o Coordenador-Geral da CGTI autorizará a ETIR a iniciar, por conta própria, o tratamento e a resposta a determinadas classes de incidentes, devidamente caracterizadas e exemplificadas, seguidas dos limites de atuação, ou de comando para atuação, no processo de contorno, contenção ou solução dos respectivos incidentes classificados.

7.5 A autorização a que se refere o item 7.4 se dará por meio registrado (física ou eletronicamente) aos Coordenadores da CGTI e ao Agente Responsável pela ETIR e deverá ser publicada no ambiente de disseminação do conhecimento da CGTI.

7.6 A dedicação a atividades proativas, na forma do item 6.8, assim como a atuação por convocação, na forma do item 6.9, deverão ser acordadas entre o Agente Responsável e o respectivo supervisor de cada integrante envolvido.

8 SERVIÇOS

8.1 Reativos

8.1.1 Tratamento de Incidentes de Segurança em Redes Computacionais:

Definição e objetivo: é o serviço que consiste em receber, filtrar, classificar e responder as solicitações e os 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.

Disponibilidade: será executado por meio da ETIR quando houver detecção de um incidente por alguma unidade.

Descrição das funções e procedimentos que compõem o serviço: o Agente Responsável realizará as atividades e procedimentos de acordo com diretrizes devidamente normatizadas e de acordo com os planos da gestão de continuidade do negócio.

Metodologia:

- O Agente Responsável, conjuntamente com seus técnicos, analisará relatórios gerados por aplicativos devidamente instituídos no MCTI e, a partir de tal informação, será elaborado relatório com a ação e/ou recomendação a ser tomada.

- Tempo de tratamento: imediato.

8.1.2 Tratamento de Artefatos Maliciosos:

Definição e objetivo: é o 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.

Disponibilidade: a) será executado por meio da ETIR quando houver o requerimento por pessoa competente na sua respectiva unidade; b) será executado quando houver detecção por meio de *software* ou outra ferramenta de gestão pela ETIR.

Descrição das funções e procedimentos que compõem o serviço: o Agente Responsável realizará as atividades e procedimentos de acordo com diretrizes devidamente normatizadas e de acordo com os planos da gestão de continuidade do negócio.

Metodologia:

- O serviço será realizado de acordo com o risco em que o artefato está classificado. O tratamento se dará primeiramente em tentativa de recuperação quando for um ativo do Ministério, e de eliminação quando for objeto fora do escopo do Ministério. Será elaborado relatório sobre a referida incidência.

- Tempo de tratamento: a depender da complexidade e urgência do caso.

8.1.3 Tratamento de Vulnerabilidades:
Definição e objetivo: é o serviço que consiste em receber informações sobre vulnerabilidades, quer sejam em *hardware* ou *software*, objetivando analisar sua natureza, seu mecanismo e suas consequências e desenvolver estratégias para detecção e correção.
Disponibilidade: a) será executado por meio da ETIR quando houver o requerimento por pessoa competente na sua respectiva unidade; b) será executado antes e depois de qualquer aquisição de ativo de TI.
Descrição das funções e procedimentos que compõem o serviço: o Coordenador da Equipe Local realizará as atividades e procedimentos de acordo com diretrizes devidamente normatizadas e de acordo com os planos da gestão de continuidade do negócio.
Metodologia:

- O serviço só poderá ser requerido pelo próprio usuário, por sua chefia imediata ou hierarquicamente superior ao Agente Responsável, que emitirá relatório com a ação e/ou recomendação a ser tomada.

- Tempo de tratamento: a depender da complexidade e urgência do caso.

8.2 Proativos
8.2.1 Detecção de Intrusão:
Definição e objetivo: é o serviço que consiste na análise do histórico de dispositivos que detectam as tentativas de intrusões em redes de computadores, com vistas a identificar e iniciar, mediante autorização, 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 e, ainda, possibilitar envio de alerta em consonância com o padrão de comunicação previamente definido entre ETIR (MCTI) e o CTIR GOV.
Disponibilidade: será executado quando houver o requerimento por pessoa competente na sua respectiva unidade através da ETIR e quando houver indícios de acesso não autorizado;
Descrição das funções e procedimentos que compõem o serviço: a Equipe realizará as atividades e procedimentos de acordo com diretrizes devidamente normatizadas e com a legislação vigente.
Metodologia:

- A Equipe analisará o ambiente e/ou os ativos envolvidos e emitirá relatório sobre a invasão.

- Tempo de tratamento: a depender da complexidade e urgência do caso.

9 DISPOSIÇÕES GERAIS

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