ANEXO I

Portaria MCTIC nº GSIC/MCTIC nº 5.357/2017

INSTITUIÇÃO DA EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS (ETIR) NO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES (MCTIC)

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 Portaria nº 4.711, de 18 de agosto de 2017 que instituiu a Política de Segurança da Informação e Comunicações do MCTIC.

2 - DEFINIÇÕES

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

2.1.1 Artefato malicioso: 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;

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

2.1.3 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;

2.1.4 ETIR: Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

2.1.5 Incidente de Segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança em sistemas de computação ou redes de computadores e que interrompa ou impacte a operação de um serviço, afetando aspectos como funcionalidade, performance ou disponibilidade;

2.1.6 Serviço: conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

2.1.7 Tratamento de Vulnerabilidades: 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;

2.1.8 Vulnerabilidade: qualquer fragilidade dos sistemas computacionais e redes de computadores que permita a exploração maliciosa e acessos indesejáveis ou não autorizados.

3 - MISSÃO

É missão da ETIR facilitar, coordenar e executar as atividades de tratamento e resposta a incidentes em redes computacionais no ambiente do MCTIC, tendo como objetivos básicos:

a) monitorar as redes computacionais;

b) detectar e analisar ataques e intrusões;

c) tratar incidentes de segurança da informação;

d) identificar vulnerabilidades e artefatos maliciosos;

e) recuperar sistemas de informação;

f) promover a cooperação com outras equipes, bem como participar de fóruns e redes nacionais e internacionais relativos à Segurança da Informação e Comunicações.

4 - PÚBLICO ALVO E PARTES ENVOLVIDAS

4.1 A ETIR atenderá a todos os usuários de serviços computacionais do MCTIC, preferencialmente por chamado registrado eletronicamente, por meio da Central de Serviços do Ministério ou por intermédio de recebimento de mensagens eletrônicas para um endereço específico de email.

4.2 Os sistemas de informação mencionados nesta norma são somente aqueles sob a tutela da Diretoria de Tecnologia da Informação (DTI) do MCTIC. O tratamento de incidentes de informação relacionados com equipamentos de terceiros não faz parte do escopo desta norma.

4.3 A ETIR deverá comunicar a ocorrência de incidente de segurança aos superiores imediatos, ao Gestor de Segurança da Informação e Comunicações (GSIC), proprietário e custodiante do ativo, assim como ao CTIR Gov, conforme procedimentos a serem definidos pelo próprio Centro, com vistas a permitir que sejam dadas soluções integradas para a Administração Pública Federal (APF).

5 - ESTRUTURA ORGANIZACIONAL

5.1 A ETIR funcionará como um grupo de trabalho permanente, multidisciplinar e de atuação primordialmente reativa, vinculada à Secretaria Executiva, composta por integrantes da DTI, instituída e coordenada pelo Gestor de Segurança da Informação e Comunicações.

5.2 A ETIR será formada por membros da DTI, preferencialmente servidores efetivos, que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais.

5.3 A ETIR será formada por 5 (cinco) integrantes:

5.3.1 3 (três) servidores da Coordenação-Geral de Serviços de Tecnologia da Informação (CGTI), um deles designado Agente Responsável;

5.3.2 2 (dois) servidores da Coordenação-Geral de Sistemas (CGSI).

5.4 O Agente Responsável será o Coordenador-Geral de Serviços de Tecnologia da Informação (CGTI) da DTI.

5.5 Os demais integrantes da ETIR serão indicados pelo Diretor de Tecnologia da Informação e designados em portaria específica.

5.6 Para cada membro da ETIR deverá ser designado um substituto que deverá ser treinado e orientado para a realização das tarefas e atividades da ETIR.

5.7 Os integrantes da ETIR exercerão suas funções regulares, não havendo necessidade de dedicação exclusiva.

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

5.9 O Agente Responsável será 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.

6 - PAPEIS E RESPONSABILIDADES

6.1 Os papéis previstos na ETIR são:

6.1.1 Gestor de Segurança da Informação e Comunicações;

6.1.2 Agente Responsável da ETIR;

6.1.3 Integrantes da ETIR.

6.2 Compete ao Gestor de Segurança da Informação e Comunicações:

6.2.1 instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), em conformidade com a Norma Complementar nº 05/IN01/DSIC/GSIPR;

6.2.2 designar os integrantes da ETIR;

6.2.3 coordenar a instituição, implementação e manutenção das condições necessárias à operação da ETIR;

6.2.4 realizar interlocução com o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR GOV);

6.2.5 promover a capacitação e o aperfeiçoamento técnico dos membros da ETIR;

6.2.6 aprovar mudanças no catálogo de serviços da ETIR.

6.3 Compete ao Agente Responsável da ETIR:

6.3.1 estabelecer os procedimentos operacionais, gerenciar as atividades e distribuir tarefas para a ETIR;

6.3.2 assistir o CTIR GOV com informações necessárias à atualização e manutenção das bases de dados de incidentes do Governo Federal.

6.3.2 ser interface com o CTIR GOV, juntamente com o Gestor de Segurança da Informação e Comunicações.

6.4 Compete aos Integrantes da ETIR:

6.4.1 receber, analisar, classificar e responder às notificações e atividades relacionadas a incidentes de segurança em redes computacionais, além de armazenar registros para formação de séries históricas como subsídio estatístico;

6.4.2 exercer outras atividades que lhe forem cometidas no seu campo de atuação.

7 - MODELO DE IMPLEMENTAÇÃO

7.1 A ETIR, estabelecida com referência a NC05/IN01/DSIC/GSIPR/2009, seguirá o Modelo 1, "Utilizando a equipe de Tecnologia da Informação – TI" e possuirá autonomia Completa.

7.1.1 Nesse modelo, as funções e serviços de tratamento de incidente deverão ser realizadas, preferencialmente, por administradores de rede ou de segurança, administradores de banco de dados, administradores de rede, analistas de suporte ou quaisquer outras pessoas com conhecimento técnico comprovado na área de segurança da informação.

7.2 Tendo plena autonomia, a ETIR poderá conduzir o seu público alvo para realizar as ações ou as medidas necessárias para reforçar a resposta ou a postura da organização na recuperação de incidentes de segurança, sem depender de níveis superiores de gestão.

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

7.3 Extraordinariamente, o Agente Responsável poderá convocar representantes de outras unidades da DTI/MCTIC para atuar em tratamento e resposta de determinado incidente de segurança.

7.3.1 A ETIR poderá contar com suporte operacional de terceiros para execução de suas atribuições desde que haja previsão legal.

8 - CATÁLOGO DE SERVIÇOS DA ETIR

8.1 Os serviços a serem providos pela ETIR estão listados no Anexo II.

8.2 Os serviços reativos da ETIR terão prioridade sobre os serviços proativos.

8.3 O catálogo de serviços pode ser revisto e atualizado a qualquer momento.

8.4 Atualizações no catálogo estão sujeitas à aprovação do Gestor de Segurança da Informação e Comunicações.

ANEXO II

CATÁLOGO DE SERVIÇOS DA EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS (ETIR)

1- SERVIÇOS DA ETIR

Os serviços a serem providos pela ETIR do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) são:

1.1 Tratamento de Incidentes de Segurança em Redes Computacionais;

1.2 Tratamento de Artefatos Maliciosos;

1.3 Tratamento de Vulnerabilidades;

1.4 Detecção de Intrusão.

2 Do Serviço de Tratamento de Incidentes de Segurança em Redes Computacionais

2.1 Definição e objetivo:

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.

2.2 Tipo do serviço:
Reativo.

2.3 Disponibilidade do serviço:

Deverá ser executado por meio da ETIR quando houver detecção de um incidente por alguma unidade.

2.4 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 a Política de Continuidade de Negócio instituída para o Ministério.

2.5 Metodologia:

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

2.6 Tempo de tratamento:

Imediato.

3 Do Serviço de Tratamento de Artefatos Maliciosos

3.1 Definição e objetivo:

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.

3.2 Tipo do serviço:

Reativo.

3.3 Disponibilidade do serviço:

O serviço deverá ser executado pela ETIR quando houver o requerimento do usuário ou quando houver detecção por meio de software ou outra ferramenta de gestão.

3.4 Descrição das funções e procedimentos que compõem o serviço:

A Equipe realizará as seguintes atividades:

3.4.1 recebimento informações ou cópia de artefato malicioso que foi utilizado no ataque, ou em qualquer atividade desautorizada ou maliciosa;

3.4.2 análise do artefato malicioso, incluindo busca e natureza do artefato, seu mecanismo, versão e objetivo;

3.4.3 desenvolvimento de uma estratégia para detecção, remoção e defesa.

3.5 Metodologia:

3.5.1 O serviço será realizado de acordo com o risco em que o artefato está classificado.

3.5.2 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.

3.5.3 Será elaborado relatório sobre a referida incidência.

3.6 Tempo de tratamento:
A depender da complexidade e urgência do caso.

4 Do Serviço de Tratamento de Vulnerabilidades

4.1 Definição e objetivo:
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.

4.2 Tipo do serviço:
Reativo.

4.3 Disponibilidade do serviço:
O serviço deverá ser executado pela ETIR quando houver o requerimento do usuário ou Agente Responsável e antes e depois de qualquer aquisição de ativo de tecnologia da informação.

4.4 Descrição das funções e procedimentos que compõem o serviço:
O serviço contemplará as seguintes atividades:

4.4.1 recebimento de informações sobre vulnerabilidades em hardware ou software;

4.4.2 análise de sua natureza, seu mecanismo e suas consequências;

4.4.3 desenvolvimento de estratégias para detecção e correção (emissão de relatório).

4.5 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.

4.6 Tempo de tratamento:
A depender da complexidade e urgência do caso.

5 Do Serviço da Detecção de Intrusão

5.1 Definição e objetivo:
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 ETIR do MCTIC e o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal – CTIR GOV.

5.2 Tipo do serviço:
Proativo.

5.3 Disponibilidade do serviço:
O serviço deverá ser executado quando houver o requerimento por pessoa competente na sua respectiva unidade através da ETIR e quando houver indícios de acesso não autorizado.

5.4 Descrição das funções e procedimentos que compõem o serviço:
A Equipe realizará as seguintes atividades:

5.4.1 análise periódica no histórico (log) de dispositivos que detectam 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;

5.4.2 identificação de eventos com características pré-definidas que possam levar a uma possível intrusão;

5.4.3 envio de alerta em consonância com o padrão de comunicação previamente definido entre a ETIR/MCTIC e o CTIR GOV;

5.4.4 emissão de relatórios sobre a invasão descrevendo o ambiente e/ou ativos envolvidos.

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

5.6 Tempo de tratamento:
A depender da complexidade e urgência do caso.