Número da Norma Complementar	Revisão	Emissão	Folha
05/CSIC/MCTIC	00		1/5

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES
Secretaria Executiva
Comitê de Segurança da Informação e Comunicações

DIRETRIZES PARA O SERVIÇO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDES COMPUTACIONAIS

ORIGEM

Comitê de Segurança da Informação e Comunicações (CSIC).

REFERÊNCIA NORMATIVA

Portaria nº 4.711, de 18 de agosto de 2017 – Posic/MCTIC.
Portaria nº 5357, de 12 de setembro de 2017 – Institui a ETIR/MCTIC.
Norma Complementar 08/IN01/DSIC/GSIPR, de 19 de agosto de 2010.
Norma Complementar 21/IN01/DSIC/GSIPR, de 08 de outubro de 2014.
ABNT NBR ISO/IEC 27001:2013.
ABNT NBR ISO/IEC 27002:2013.

CAMPO DE APLICAÇÃO

Esta Norma Complementar aplica-se aos órgãos de assistência direta e imediata ao Ministro de Estado; aos órgãos específicos singulares e às unidades descentralizadas deste Ministério.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há.

APROVAÇÃO

Gilberto Kassab
Ministro

Número da Norma Complementar	Revisão	Emissão	Folha
05/CSIC/MCTIC	00		2/5

1 OBJETIVO

Estabelecer diretrizes para o serviço de tratamento de incidentes de segurança em redes computacionais no âmbito do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC).

2 TERMOS E DEFINIÇÕES

Para os efeitos desta norma, aplicam-se os seguintes termos e definições:

2.1 **Ativo de Informação** - os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

2.2 **Agente Responsável pela ETIR** - servidor público ocupante de cargo efetivo ou militar de carreira de órgão da Administração Pública Federal (APF), direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

2.3 **Central de Serviços** - equipe responsável pelos serviços de suporte técnico de tecnologia da informação do MCTIC. Normalmente está associada aos colaboradores pertencentes ao contrato de sustentação da infraestrutura de rede do órgão.

2.4 **Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR Gov)** - centro de tratamento subordinado ao Departamento de Segurança de Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República - DSIC/GSI/PR.

2.5 **Equipe de Monitoramento de Rede** - equipe responsável pelo monitoramento da infraestrutura do órgão. Normalmente está associada aos colaboradores pertencentes ao contrato de sustentação da infraestrutura de rede do MCTIC.

2.6 **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR)** - grupo de pessoas com a responsabilidade de receber, analisar e responder à notificações e atividades relacionadas à incidentes de segurança em redes computacionais.

2.7 **Endereço IP (Internet Protocol)** - refere-se ao conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores.

2.8 **Evidência** - informação ou dado, armazenado ou transmitido eletronicamente que pode ser reconhecida como parte de um evento.

2.9 **Gestor de Segurança da Informação e Comunicações** - autoridade responsável por coordenar e instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR).

2.10 **Incidente de Segurança** - qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança da informação 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.

2.11 **Informação Sigilosa** - informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo.

2.12 **Metadados** - Conjunto de dados que descrevem outros dados.

2.13 **Preservação de evidência** - é o processo que compreende a salvaguarda das evidências e dos dispositivos, de modo a garantir que os dados ou metadados não sofram alteração, preservando-se a integridade e a confidencialidade das informações.

2.14 **Serviço de Tratamento de Incidentes de Segurança em Redes Computacionais** - 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.

2.15 **Software** - programa de computador e seus respectivos dados de configuração.

2.16 **Usuário** - agente público, colaborador ou estagiário que faz uso dos recursos de tecnologia da informação, rede e telefonia do MCTIC.

3 DISPOSIÇÕES GERAIS

A ETIR deve observar e adotar, no mínimo, os seguintes aspectos e procedimentos:

3.1 Registro de incidentes de segurança em redes de computadores: todos os incidentes notificados ou detectados devem ser registrados, adotando o procedimento previsto no item 4.2 desta Norma, com a finalidade de assegurar o registro histórico das atividades da ETIR;

3.2 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;

3.3 Recursos disponíveis: a ETIR deve possuir os recursos materiais, tecnológicos e humanos, suficientes para prestar os seus serviços;

3.4 Capacitação dos membros da ETIR: os membros da ETIR devem estar capacitados para operar os recursos disponíveis para a condução dos seus serviços;

3.5 Durante o gerenciamento de incidentes de segurança em redes de computadores, havendo indícios de ilícitos criminais, a ETIR tem como dever:

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

3.5.2 Observar os procedimentos para preservação das evidências, conforme Norma Complementar nº 06/CSIC/MCTIC;

3.6 Priorizar a continuidade dos serviços da ETIR e da missão institucional da organização, observando os procedimentos previstos no item 3.5.2 desta Norma Complementar.

4 PROCEDIMENTOS

4.1 Identificação de Incidente de Segurança

4.1.1 Todos os usuários que tenham conhecimento de incidentes de segurança devem notificar a Central de Serviços por meio de abertura de chamado em ferramenta específica, pelo endereço de e-mail "suporte@mctic.gov.br" ou pelo telefone da Central de Serviços, responsável pela prestação de serviço de suporte de tecnologia da informação.

4.1.2 Os incidentes de segurança identificados pela ETIR, pela Central de Serviços ou pela Equipe de Monitoramento de Rede devem ser registrados diretamente em ferramenta específica, conforme item 4.2 desta Norma.

4.1.3 Os incidentes de segurança identificados por softwares especializados deverão ser registrados em ferramenta específica, conforme item 4.2 desta Norma.

4.2 Registro de Incidente de Segurança

4.2.1 O registro do incidente de segurança deverá ser realizado em ferramenta específica, disponibilizada pela Diretoria de Tecnologia da Informação (DTI).

4.2.2 A ferramenta que trata o item anterior será a mesma utilizada para o controle dos chamados pela Central de Serviços.

4.2.3 O registro deverá conter as seguintes informações:

a) identificação do usuário que registrou o incidente de segurança;

b) descrição dos fatos do incidente de segurança;

c) data, hora e fuso horário do incidente de segurança;

d) outras informações relevantes sobre o incidente de segurança.

4.3 Análise do Incidente de Segurança

4.3.1 Após o registro, a ETIR deverá ser notificada do registro do incidente pelo endereço eletrônico "etir@mctic.gov.br".

4.3.2 Caso a ETIR confirme que a ocorrência registrada é um incidente de segurança, deverá identificar os ativos de informação e serviços afetados e mensurar os impactos do incidente nos ativos de informação, considerando os critérios de confidencialidade, integridade, disponibilidade e autenticidade.

4.3.3 Após a mensuração dos impactos, deve-se classificar, priorizar e atribuir as responsabilidades para o tratamento do incidente.

4.4 Tratamento do incidente de segurança

4.4.1 A ETIR deve acompanhar a resolução do incidente de segurança, verificando se o tratamento do incidente segue os processos, os métodos e as normas estabelecidas.

4.4.2 A ETIR deve garantir a recuperação dos ativos de informação e serviços impactados em conformidade com os planos de recuperação, quando disponíveis.

4.4.3 O conhecimento adquirido na resolução dos incidentes deve ser registrado em base de conhecimento específica, no intuito de aprimorar a segurança do órgão e compartilhar as informações com o CTIR Gov.

4.4.4 As evidências do incidente devem ser armazenadas seguindo o disposto na Norma Complementar nº 06/CSIC/MCTIC.

4.4.5 A ETIR deve adotar, após a resolução do incidente de segurança, as providências necessárias para eliminar ou minimizar a possibilidade de uma nova ocorrência do incidente.

4.5 Comunicação do Incidente de Segurança

4.5.1 O agente responsável pela ETIR deverá comunicar a ocorrência de incidente de segurança ao Gestor de Segurança da Informação e Comunicações (GSIC), ao proprietário e ao custodiante do ativo de informação e ao Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR Gov, conforme procedimentos a serem definidos pelo próprio CTIR Gov, com vistas a permitir que sejam dadas soluções integradas para a APF, bem como a geração de estatísticas.

4.5.2 A comunicação à autoridade com atribuição para apurar os fatos do incidente de segurança deverá obedecer ao disposto na Norma Complementar nº 06/CSIC/MCTIC.

5 VIGÊNCIA

Esta Norma Complementar entra em vigor na data de sua publicação.