Número da Norma Complementar	Revisão	Emissão	Folha
04/Port. 04/CGD/MDIC	00	/DEZ/16	1/5

MINISTÉRIO DA INDÚSTRIA, COMÉRCIO EXTERIOR E SERVIÇOS
Comitê de Governança Digital

Gerenciamento de Incidentes em Redes no Âmbito do Ministério da Indústria, Comércio Exterior e Serviços (MDIC)

ORIGEM

Comitê de Governança Digital (CGD) do MDIC

REFERÊNCIA NORMATIVA E BIBLIOGRÁFICAS

Instrução Normativa GSI Nº 1, de 13 de junho de 2008
Norma Complementar nº 05/IN01/DSIC/GSIPR
Norma Complementar nº 08/IN01/DSIC/GSIPR
Norma Complementar nº 21/IN01/DSIC/GSIPR

CAMPO DE APLICAÇÃO

Esta norma se aplica a todos os colaboradores do MDIC.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há

APROVAÇÃO

MARCOS JORGE DE LIMA
Presidente do Comitê de Governança Digital

Número da Norma Complementar	Revisão	Emissão	Folha
04/Port. 04/CGD/MDIC	00	/DEZ/16	2/5

1. OBJETIVO

Instituir e regulamentar o funcionamento da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR, do Ministério da Indústria, Comércio Exterior e Serviços – MDIC, em complemento à diretriz estabelecida pela alínea "a" do inciso II do art. 7º da Política de Segurança da Informação e Comunicações – POSIC – do MDIC.

2. DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:

2.1. 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 ETIR;

2.2. 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;

2.3. 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;

2.4. 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;

2.5. 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;

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

2.7. 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;

2.8. 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;

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

Número da Norma Complementar	Revisão	Emissão	Folha
04/Port. 04/CGD/MDIC	00	/DEZ/16	3/5

3. MISSÃO

A ETIR do MDIC 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 MDIC, atuando também de forma proativa com o objetivo de minimizar vulnerabilidades e ameaças que possam comprometer o negócio da Instituição.

4. COMUNIDADE OU PÚBLICO ALVO

4.1. Todos os servidores e colaboradores que exercem suas atividades no âmbito do MDIC;

4.2. Demais equipes de resposta a incidentes de segurança da informação e comunicações da Administração Pública Federal;

4.3. CTIR GOV;

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

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

5. MODELO DE IMPLEMENTAÇÃO

5.1. O MDIC adotará o modelo de implementação da ETIR proposto pelo item 7.1 da Norma Complementar nº 05/IN01/DSIC/GSIPR, qual seja, **Modelo 1 – Utilizando a equipe de Tecnologia da Informação – TI.**

5.2. De acordo com a referida norma, neste modelo não existirá um grupo dedicado exclusivamente às funções de tratamento e resposta a incidentes de Rede. A Equipe será formada a partir dos membros das equipes de TI do próprio órgão ou entidade, que além de suas funções regulares passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais. Neste modelo as funções e serviços de tratamento de incidente deverão ser realizadas, preferencialmente, por administradores de rede ou de sistema ou, ainda, por peritos em segurança.

5.3. A Equipe que utilizar este modelo desempenhará suas atividades, via de regra, de forma reativa, sendo desejável, porém, que o Agente Responsável pela ETIR atribua responsabilidades para que os seus membros exerçam atividades pró-ativas.

6. ESTRUTURA ORGANIZACIONAL

6.1. A estrutura organizacional da ETIR será composta pelo Agente Responsável e por um ou mais Membros da Equipe.
6.2. 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 ETIR.

6.3. O Membro da Equipe será Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores e demais atividades descritas nesta norma.

6.4. Os servidores que compõem a ETIR deverão ser nomeados por meio de portaria CGD, por indicação do Gestor de Segurança da Informação e Comunicações.

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

6.6. O Gestor de Segurança da Informação e Comunicações da organização será o responsável por definir, junto à área de gestão de pessoas do MDIC, as necessidades de capacitação e o aperfeiçoamento técnico dos membros da Equipe.

7. AUTONOMIA

7.1. A ETIR trabalhará com autonomia compartilhada e em acordo com os outros setores da organização a fim de participar do processo de tomada de decisão sobre quais medidas devam ser adotadas.

7.2. A Equipe poderá recomendar os procedimentos a serem executados ou as medidas de recuperação durante um ataque e discutirá as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas) com o Gestor de Segurança da Informação e Comunicações.

8. ATRIBUIÇÕES

8.1. Garantir que os incidentes em Redes Computacionais da Rede de Computadores do MDIC sejam monitorados e tratados;

8.2. Adotar procedimentos de feedback para assegurar que os usuários que comuniquem incidentes de segurança da informação e comunicações sejam informados dos procedimentos adotados;

8.3. Apoiar os treinamentos relacionados à SIC fornecendo casos práticos de incidentes de segurança, garantindo-se a confidencialidade e devidos níveis de sigilo, sobre o que poderia acontecer, como reagir a tais incidentes e como evita-los no futuro;

8.4. Recolher provas o quanto antes após a ocorrência de um incidente de SIC;

8.5. Executar uma análise crítica sobre os registros de falha para assegurar que estas foram satisfatoriamente resolvidas;

8.6. Investigar as causas dos incidentes de SIC;

8.7. Submeter ao Gestor de Segurança da Informação e Comunicações as ocorrências de violação às normas de segurança da informação e comunicações do MDIC;

8.8. Implementar mecanismos para permitir a quantificação e monitoração dos tipos, volumes e custos de incidentes e falhas de funcionamento;

8.9. Indicar a necessidade de controles para limitar a frequência e os danos de futuras ocorrências de incidentes de segurança em redes de computadores;

8.10. Emitir relatório periódico contendo resumo das ocorrências de incidentes de segurança para apresentação ao CSIC;

8.11. Notificar o Gestor de Segurança da Informação e Comunicações a respeito dos eventos e incidentes de segurança da informação comunicações na rede de computadores do MDIC que ensejem aplicação de penalidades previstas em normativos de SIC; e

8.12. Comunicar a ocorrência de incidentes de segurança em redes de computadores ao CTIR Gov, conforme procedimentos definidos pelo próprio CTIR Gov, com vistas a permitir que sejam dadas soluções integradas para a Administração Pública Federal, bem como a geração de estatísticas.

9. DISPOSIÇÕES GERAIS

9.1. Os servidores e colaboradores devem comunicar a ETIR, o mais breve possível, toda e qualquer falha, anomalia, ameaça ou vulnerabilidade identificada, mesmo que seja apenas uma suspeita.

9.2. O canal de comunicação com a ETIR é o e-mail cgti.seguranca@mdic.gov.br.

9.3. A ETIR deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede orientados pelo CTIR GOV.

9.4. A ETIR poderá usar as melhores práticas de mercado, desde que não conflitem com os dispositivos desta Norma Complementar.

9.5. A troca de informações e a forma de comunicação entre as ETIR, e entre estas e o CTIR GOV, serão formalizadas caso a caso, se necessário, por Termo de Cooperação Técnica.

10. VIGÊNCIA

Esta Norma entra em vigor na data da sua publicação.