Número da Norma Complementar	Revisão	Emissão	Folha
08/IN01/DSIC/GSIPR	00	24/AGO/10	1/5

PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações

GESTÃO DE ETIR: DIRETRIZES PARA GERENCIAMENTO DE INCIDENTES EM REDES COMPUTACIONAIS NOS ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

- Art. 6º da Lei nº 10.683, de 28 de maio de 2003.
- Art. 8º do Decreto nº 6.931, de 11 de junho de 2009.
- Art. 8º do Anexo I do Decreto nº 3.505, de 13 de junho de 2000.
- Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008.
- NC 05 do Gabinete de Segurança Institucional, de 14 de agosto de 2009.
- Incisos II e IV do art. 37 da Portaria nº 13 do Gabinete de Segurança Institucional, de 04 de agosto de 2006.

CAMPO DE APLICAÇÃO

Esta Norma Complementar se aplica no âmbito da Administração Pública Federal, direta e indireta.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há

APROVAÇÃO

RAPHAEL MANDARINO JUNIOR
Diretor do Departamento de Segurança da Informação e Comunicações

1 OBJETIVO

Disciplinar 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.

2 CONSIDERAÇÕES INICIAIS

2.1 O gerenciamento de incidentes de segurança em redes de computadores requer especial atenção da alta administração dos órgãos e entidades da APF.

2.2 A troca de informações sobre o gerenciamento de incidentes de segurança em redes de computadores entre as ETIR e a Coordenação Geral de Tratamento de Incidentes de Segurança em Redes de Computadores - CGTIR permite, entre outras coisas:

2.2.1 promover o intercâmbio científico-tecnológico relacionado a incidentes de segurança em redes de computadores;

2.2.2 apoiar órgãos e entidades da APF nas atividades de gerenciamento e tratamento de incidentes de segurança em redes de computadores, quando necessário;

2.2.3 monitorar e analisar tecnicamente os incidentes de segurança em redes de computadores da APF, permitindo a criação de métricas e/ou alertas;

2.2.4 implementar mecanismos que permitam a avaliação dos danos ocasionados por incidentes de segurança em redes de computadores da APF;

2.2.5 apoiar, incentivar e contribuir, no âmbito da APF, para a capacitação no tratamento de incidentes de segurança em redes de computadores.

3 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

Conforme disposto no inciso II do art. 3º da Instrução Normativa nº 01, de 13 de Junho de 2008, do Gabinete de Segurança Institucional, compete ao Departamento de Segurança da Informação e Comunicações - DSIC, estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

4 CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar serão adotados os conceitos e definições descritos na Norma Complementar nº 05/IN01/DSIC/GSIPR, publicada no Diário Oficial da União em 17 de agosto de 2009.

5 RESPONSABILIDADE

O Agente Responsável, designado no documento de criação da ETIR, é o responsável pela ETIR do seu órgão ou entidade, bem como pelo relacionamento com o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR Gov.

6 RELACIONAMENTOS DA ETIR

A ETIR comunicará a ocorrência de incidentes de segurança em redes de computadores 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.

7 GESTÃO DOS SERVIÇOS

Para a definição dos serviços que serão prestados cada órgão deverá observar as suas necessidades e limitações, a missão, o modelo de implementação adotado e a autonomia da ETIR;

7.1 Recomenda-se que a ETIR defina os serviços a serem oferecidos à sua comunidade e, na medida em que forem oferecidos, que o sejam de forma gradativa e de acordo com a maturidade da equipe;

7.2 Além do serviço de tratamento de incidentes de segurança em redes de computadores, a ETIR poderá oferecer à sua comunidade um ou mais dos serviços listados a seguir, sem prejuízo de outros requisitados, desde que em consonância com normas e legislações referentes ao gerenciamento de incidentes de segurança em redes de computadores:

7.2.1 Tratamento de artefatos maliciosos;

7.2.2 Tratamento de vulnerabilidades;

7.2.3 Emissão de alertas e advertências;

7.2.4 Anúncios;

7.2.5 Prospecção ou monitoração de novas tecnologias;

7.2.6 Avaliação de segurança;

7.2.7 Desenvolvimento de ferramentas de segurança;

7.2.8 Detecção de intrusão;

7.2.9 Disseminação de informações relacionadas à segurança;

7.3 Descrição, puramente exemplificativa, dos possíveis serviços de tratamento de incidentes de

segurança em redes de computadores, não esgotando a possibilidade de implementação de outros serviços inerentes às peculiaridades da ETIR:

7.3.1 Tratamento de artefatos maliciosos - Este serviço prevê o recebimento de informações ou cópia do artefato malicioso que foi utilizado no ataque, ou em qualquer outra atividade desautorizada ou maliciosa. Uma vez recebido o artefato 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 contra estes artefatos;

7.3.2 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;

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

7.3.4 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;

7.3.5 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;

7.3.6 Avaliação de segurança - Este serviço consiste em efetuar uma análise detalhada da infraestrutura de segurança em redes de computadores 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, varredura da rede e testes de penetração;

7.3.7 Desenvolvimento de ferramentas de segurança - Este serviço consiste no desenvolvimento de qualquer ferramenta nova específica de tratamento de incidentes de segurança em redes de computadores, para a ETIR ou para comunidade;

7.3.8 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 e o CTIR Gov;

7.3.9 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.

8 DISPOSIÇÕES GERAIS

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

8.1 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;

8.2 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;

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

8.4 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;

8.5 Durante o gerenciamento de incidentes de segurança em redes de computadores, havendo indícios de ilícitos criminais, as ETIR têm como dever, sem prejuízo do disposto no item 6 desta Norma Complementar e do item 10.6 da Norma Complementar nº 05/IN01/DSIC/GSIPR:

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

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

8.5.3 Priorizar a continuidade dos serviços da ETIR e da missão institucional da organização, observando os procedimentos previstos no item 8.5.2.

9 VIGÊNCIA

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