MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES AGÊNCIA ESPACIAL BRASILEIRA	Número da Norma Complementar à POSIC/AEB	Revisão	Emissão	Folha
	02/GTPOSIC/AEB	-	-	01/09
TRATAMENTO DE INCIDENTES DE REDE				

ORIGEM

Grupo de Trabalho da Política de Segurança da Informação e Comunicações da AEB

REFERÊNCIA NORMATIVA

- Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
- Norma Complementar nº 01 IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações.
- Norma NBR/ISO/IEC 27.005:2011, que estabelece diretrizes para o gerenciamento dos riscos de Segurança da Informação-SI.
- Norma Complementar nº 05/IN01/CSIC/GSIPR, que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal.
- Norma Complementar nº 07/IN01/CSIC/GSIPR, que estabelece diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
- Norma Complementar nº 08/IN01/CSIC/GSIPR, que estabelece diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.
- Lei nº 12.737/2012, de 30 de novembro de 2012 - dispõe sobre a tipificação criminal de delitos informáticos.
- ISO/IEC 27037:2012 – "*Information the technology" – "Security Techniques – Guidelines for Identification, collection, acquisition, and preservation of digital evidence*".
- RFC – "*Request for Comments": 3227 – February 2002 – "Guidelines for Evidence Collection and Archiving*".
- Portaria SLTI/MP nº 5 de 14 de junho de 2005: e-PING – Padrões de Interoperabilidade de Governo eletrônico.
- Decreto nº 7.845, de 14 de novembro de 2012 - regulamenta procedimentos para o credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo no âmbito do Poder Executivo federal, e dispõe sobre o Núcleo de Segurança e Credenciamento.

CAMPO DE APLICAÇÃO

Esta Norma se aplica no âmbito da Agência Espacial Brasileira - AEB

SUMÁRIO

APROVAÇÃO
JOSÉ RAIMUNDO BRAGA COELHO
Presidente da Agência Espacial Brasileira

1. OBJETIVO

- Disciplinar a criação, na AEB, da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR;
- 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 da AEB.
- Estabelecer, na AEB, as Diretrizes para o registro de eventos, coleta e preservação de evidências de incidentes de segurança em redes.

2. CONSIDERAÇÕES INICIAIS

2.1. O gerenciamento de incidentes de segurança em redes de computadores requer especial atenção da alta administração da AEB, visto que é parte crítica para garantir a confidencialidade, integridade e disponibilidade dos serviços executados pela AEB.

2.2. Será definida uma equipe para tratamento e resposta aos incidentes em redes computacionais, seguindo critérios a serem definidos pela área de TI da AEB, nomeada ETIR, a fim de receber, analisar e responder às notificações e atividades relacionadas aos incidentes de segurança em redes computacionais na AEB.

2.3. 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, do GSI/PR, permite, entre outras coisas:

I. Promover o intercâmbio científico-tecnológico relacionado a incidentes de segurança em redes de computadores;
II. Apoiar as atividades de gerenciamento e tratamento de incidentes de segurança em redes de computadores, quando necessário;
III. Monitorar e analisar tecnicamente os incidentes de segurança em redes de computadores da AEB, permitindo a criação de métricas e/ou alertas;
IV. Implementar mecanismos que permitam a avaliação dos danos ocasionados por incidentes de segurança em redes de computadores da AEB; e
V. Apoiar, incentivar e contribuir, no âmbito da AEB, para a capacitação no tratamento de incidentes de segurança em redes de computadores.

2.4. Os incidentes de segurança da informação devem ser gerenciados e registrados.

3. CONCEITOS E DEFINIÇÕES

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

Agente público: todo aquele que, por força de lei, contrato ou de qualquer ato jurídico, preste serviços de natureza permanente, temporária ou excepcional, ainda que sem retribuição financeira, desde que ligado direta ou indiretamente à AEB.

Ativo de informação: qualquer pessoa, tecnologia, processo ou ambiente que processe, armazene, transporte ou descarte informação institucional.

Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

Comitê de Segurança da Informação e Comunicações: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito da AEB.

Sigilo: é a condição de algo que é mantido como oculto e secreto, fazendo com que poucas pessoas saibam da sua existência.

Diretriz: Conjunto de instruções ou indicações que orientem o que deve ser feito para se alcançar os objetivos estabelecidos na POSIC/AEB.

Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais: grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores.

Incidentes de segurança: qualquer evento, indesejado ou inesperado, que comprometa as operações ou ameace a segurança da informação.

Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

Segurança da Informação e Comunicações: ações que objetivem viabilizar e assegurar a disponibilidade, a integridade, o sigilo e a autenticidade das informações

4. DIRETRIZES GERAIS

4.1. Implementação da ETIR

a) Fica instituída a figura do **Agente Responsável** que será um Servidor Público ocupante de cargo efetivo incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais e fazer a interface com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV, além de criar, gerenciar e distribuir as tarefas para a ETIR. Este Agente será, preferencialmente, o responsável pelo setor de informática da AEB;

b) O modelo de implementação da ETIR, a ser utilizado inicialmente, será o modelo nº 1 (Utilizando a equipe de Tecnologia da Informação – TI) preconizado na Norma Complementar nº 05/IN01/DSIC/GSIPR, datada de 14/08/2009. A equipe irá trabalhar de maneira reativa. Entretanto, o Agente Responsável pode delegar responsabilidade para que a ETIR exerça tarefas proativas;

c) As ações reativas incluem recebimento de notificações de incidentes, orientação no reparo a danos, e análise de sistemas comprometidos buscando causas, danos e responsáveis;

d) As ações proativas se dão pela não necessidade de notificação, isto é, a ETIR tem o dever de agir

no tratamento de riscos, sempre que possível previamente comunicado a Autoridade de Monitoramento da AEB, nomeado pelo presidente da AEB através da Portaria nº 16 de 7 de março de 2012, o motivo da ação, para que seja preservada a Segurança da Informação.

e) A ETIR terá autonomia plena, em escopo restrito, podendo conduzir o seu público alvo para realizar ações ou medidas necessárias para reforçar a resposta ou a postura da organização na recuperação de incidentes de segurança. Sendo assim, a ETIR não precisa da aprovação de níveis superiores de gestão para executar medidas de recuperação.

4.2. Competências e outras disposições

a) A ETIR terá por competências:

I. Coordenar, executar e acompanhar as atividades de tratamento e resposta a incidentes na rede corporativa da AEB;

II. Coordenar, executar e acompanhar a análise dos sistemas comprometidos buscando causas, danos e responsáveis;

III. Gerenciar contratos de prestação de serviços específicos, controlando a qualidade dos resultados de acordo com os critérios de aceitação do produto e dos serviços prestados estabelecidos através de procedimento criada pela DINF;

IV. Coordenar, executar e acompanhar a avaliação, auditoria e testes das condições de segurança da rede corporativa da AEB;

V. Coordenar, executar e acompanhar a análise dos ativos de informação e estruturas constitutivas dos ambientes de tecnologia da informação, presentes na AEB;

VI. Prestar assessoria técnica na elaboração de políticas, normas, pareceres e na especificação técnica de produtos e equipamentos direcionados à segurança da informação e comunicações;

VII. Executar outras atividades correlatas que lhe forem demandadas, desde que relacionadas à segurança da informação e ligadas ao Tratamento e Resposta de Incidentes em Redes Computacionais;

4.3. Tratamento de Incidentes

a) Os colaboradores devem estar cientes que o tratamento de incidentes visa minimizar os impactos de um incidente nos processos em curso na AEB;

b) Quaisquer falhas, anomalias, ameaças ou vulnerabilidades observadas devem ser notificadas o mais rápido possível por meio do e-mail: etir@aeb.gov.br;

c) A ETIR deverá propor, em forma de procedimento, regras para ações disciplinatórias no caso de condutas que violem as políticas estabelecidas ou que comprometam a segurança das informações da organização;

d) Cabe a ETIR obter informações qualitativas e, quando possível, quantitativas acerca dos incidentes ocorridos que descrevam: sua natureza, causas, data da ocorrência, frequência e os custos resultantes. Tais informações servem como indicadores da eficácia das políticas e da relação custo-benefício dos controles de segurança;

e) Após o levantamento dos dados do incidente, a ETIR deverá tratá-los e documentá-lo, visando manter um histórico dos incidentes e, ainda, uma cultura acerca dos mesmos. O modelo de relatório consta no Anexo A desta Norma Complementar;

f) Caso o incidente tenha como origem outro órgão da Administração Pública Federal e/ou outro país, o CTIR GOV deverá ser acionado para juntar-se a ETIR da AEB para tratar do incidente;

g) A área de Tecnologia da Informação deve estar preparada, através da utilização e fornecimento de processos, ferramentas tecnológicas e recursos humanos capacitados para garantir a integridade, disponibilidade e sigilo dos dados, levando em consideração a norma complementar nº 03 – Gestão de Risco da AEB;

5. DOS REQUISITOS PARA ADEQUAÇÃO DOS ATIVOS DE INFORMAÇÃO

a) O horário dos ativos de informação, quando for o caso, deve ser ajustado por meio de mecanismos de sincronização de tempo, de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON);
b) Os ativos de informação devem ser configurados, quando possível, de forma a registrar eventos relevantes de Segurança da Informação e Comunicação - SIC, contendo, no mínimo, os seguintes itens:
    b.1) Autenticação, tanto os bem-sucedidos quanto os malsucedidos;
    b.2) Acesso a recursos e dados privilegiados, podendo ser definidos em processos posteriores; e
    b.3) Acesso e alteração nos registros de auditoria.
c) Caso o ativo de informação não permita este tipo de registro, o mesmo deve ser mapeado e documentado sobre o tipo e formato de registro de auditoria que o sistema permita armazenar;
d) Os servidores de hospedagem de página eletrônica, bem como todo e qualquer outro ativo de informação que o permita, devem ser configurados para armazenar registros históricos de eventos (*Logs*) de forma que permita a completa identificação dos fluxos de dados;
e) Os registros devem ser armazenados pelo período mínimo de 05 (cinco) anos, sem prejuízo de outros prazos previstos em normativos específicos;

DIRETRIZES ESPECÍFICAS

São diretrizes específicas da ETIR:

a) Monitorar o sistema de abertura de chamado e mapear os riscos mais frequentes;
b) Criar históricos de monitoramento, a fim de mitigar os riscos de uma maneira mais ágil;
c) Criar campanhas de conscientização de boas práticas da utilização de ferramentas disponibilizadas pela DINF;
d) Criar procedimentos de utilização de bens e serviços de TI;
e) Subsidiar a regulação das políticas de acessos e perfis de usuários;
f) Criar ações de tratamento e resposta a incidentes em redes computacionais; e
g) Elaborar manuais e fluxo de tratamento de incidentes de rede.

6. VIGÊNCIA

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

ANEXO

RELATÓRIO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA EM REDES COMPUTACIONAIS

DADOS GERAIS:

Nº da Ocorrência/Ano: _____/_____

1. Nome do agente responsável pela preservação dos dados do incidente:
_____Matrícula: _____
Endereço eletrônico: _____ Telefone: (___) _____
2. Nome do responsável pela ETIR: _____
_____ Matrícula: _____
Endereço eletrônico: _____ Telefone: (___) _____
Nome do Órgão/Instituição: _____
Endereço: _____

DESCRIÇÃO DO INCIDENTE:

_____

_____
__
_____

_____
_____
_____

ORIGEM DO INCIDENTE OU A RAZÃO DE NÃO SER POSSÍVEL IDENTIFICÁ-LA:
_____

_____

_____

COMO FOI DETECTADO O INCIDENTE?

_____
_____
_____

QUAIS FORAM OS DADOS COLETADOS E PRESERVADOS?

_____

_____

OUTROS DADOS JULGADOS RELEVANTES:

_____
_____
_____

_____

QUAIS FORAM AS AÇÕES DE TRATAMENTO E RESPOSTA AO INCIDENTE?

_____
_____
_____
__
_____

COMO FORAM PRESERVADOS OS REGISTROS DO INCIDENTE? QUAIS AS FERRAMENTAS UTILIZADAS?

_____
_____

_____
_____

QUAL FOI O LOCAL DE ARMAZENAMENTO DAS INFORMAÇÕES PRESERVADAS?

_____

Local e data:_____, _____ /____ /_____

_____
Assinatura do agente responsável pela preservação dos dados do incidente