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

DIRETRIZES PARA O REGISTRO DE EVENTOS, COLETA E PRESERVAÇÃO DE EVIDÊNCIAS DE INCIDENTES DE SEGURANCA EM REDES

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA LEGAL E NORMATIVA

Lei nº 12.737/2012, de 30 de novembro de 2012.
Art. 6º do Código de Processo Penal.
Decreto n° 1.171, de 22 de Junho de 1994.
Decreto nº 3.505, de 13 de junho de 2000.
Decreto nº 7724, de 16 de maio de 2012.
Decreto nº 7845, de 14 de novembro de 2012.
Instrução Normativa GSI/PR nº 01/2008 e suas respectivas Normas Complementares.
Instrução Normativa GSI/PR nº 02/2013 e suas respectivas Normas Complementares.
Portaria MCT nº 293, de 11 de Maio de 2007.
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.

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

Estabelecer diretrizes para o registro, coleta e preservação de evidências de incidentes de segurança em redes computacionais dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF e a comunicação às autoridades competentes.

2 CONSIDERAÇÕES INICIAIS

2.1 É interesse do Estado e da sociedade a investigação e a responsabilização por condutas ilícitas que danifiquem ou exponham a segurança das redes e sistemas computacionais ou que possam comprometer a disponibilidade, integridade, confidencialidade e autenticidade da informação na APF.

2.2 O processo de Gestão da Segurança da Informação e Comunicações abrange as atividades de registro de eventos, coleta e preservação de evidências de incidentes de segurança em redes computacionais, o qual inclui a identificação das causas e o tratamento dos incidentes.

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 (GSI), compete ao Departamento de Segurança da Informação e Comunicações (DSIC), estabelecer normas definindo os requisitos metodológicos para a implementação da Gestão de SIC pelos órgãos e entidades da APF e previsão contida no item 8.5 da Norma Complementar 08/IN01/DSIC/GSIPR, que estabelece as diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e entidades da APF.

4 CONCEITOS E DEFINIÇÕES

Para efeito desta Norma Complementar aplicam-se os seguintes conceitos e definições:

4.1 **Acesso:** ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade.

4.2 **Agente responsável pela ETIR:** 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.

4.3 **Aquisição de evidência:** processo de coleta e cópia das evidências de incidente de segurança em redes computacionais.

4.4 **Ativos 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.

4.5 **Auditoria:** processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos.

4.6 **Autenticação:** processo de identificação das partes envolvidas em um processo.

4.7 **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.

4.8 **Autorização:** processo que visa garantir que as informações são acessíveis exclusivamente àqueles com permissão de acesso.

4.9 **Coleta de evidências de segurança em redes computacionais:** Processo de obtenção de itens físicos que contém uma potencial evidência, mediante a utilização de metodologia e ferramentas adequadas. Este processo inclui a aquisição, ou seja, a geração das cópias das mídias, ou coleção de dados que contenham evidências do incidente.

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

4.11 **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 a incidentes de segurança em redes de computadores.

4.12 **Evidência digital:** informação ou dado, armazenado ou transmitido eletronicamente, em modo binário, que pode ser reconhecida como parte de um evento.

4.13 **Incidente de segurança em redes computacionais:** é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

4.14 **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.

4.15 **Log ou Registro de Auditoria:** Registro de eventos relevantes em um dispositivo ou sistema computacional.

4.16 **Metadados**: Conjunto de dados estruturados que descrevem informação primária.

4.17 **Preservação de evidência de incidentes em redes computacionais:** 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.

4.18 **Resumo Criptográfico:** é um método criptográfico que, quando aplicado sobre uma informação, independente do tamanho desta, gera um resultado único e de tamanho fixo, também chamado de "*hash*".

4.19 **Tratamento da Informação Classificada:** conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo.

5 DOS INCIDENTES DE SEGURANÇA EM REDES COMPUTACIONAIS

Estão abrangidos nesta Norma Complementar todos os eventos contrários ao ordenamento jurídico em vigor, bem como as normas constantes da política de segurança da organização, relativos à Segurança da Informação e Comunicações (SIC), como:

a) Divulgação não autorizada de dado ou informação sigilosa contida em sistema, arquivo ou base de dados da APF, nos termos do art. 153, §1º-A do Código Penal;

b) Invasão de dispositivo informático, nos termos do art. 154-A do Código Penal;

c) Interrupção de serviço telemático ou de informação de utilidade pública, previsto no §1º do art. 266 do Código Penal;

d) Inserção ou facilitação de inserção de dados falsos, alteração ou exclusão de dados corretos nos sistemas informatizados ou bancos de dados da APF, nos termos do art. 313-A do Código Penal;

e) Modificação ou alteração por funcionário público de sistema de informação ou programa de informática sem autorização, nos termos do art. 313-B do Código Penal;

f) Distribuição, armazenamento ou conduta vinculada a pornografia infantil, nos termos dos arts. 240, 241, 241-A, 241-B, 241-C e 241-D da Lei nº 8069/90; e

g) Interceptação telemática clandestina, nos termos do art. 10 da Lei nº 9296/96.

6 DOS REQUISITOS PARA ADEQUAÇÃO DOS ATIVOS DE INFORMAÇÃO

6.1 O horário dos ativos de informação deve ser ajustado por meio de mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a "Hora Legal Brasileira (HLB)", de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).

6.2 Os ativos de informação devem ser configurados de forma a registrar todos os eventos relevantes de SIC, e no mínimo, os seguintes:

a) Autenticação, tanto os bem-sucedidos quanto os malsucedidos;

b) Acesso a recursos e dados privilegiados; e

c) Acesso e alteração nos registros de auditoria.

6.3 Os registros dos eventos previstos no item anterior devem incluir as seguintes informações:

a) Identificação inequívoca do usuário que acessou o recurso;

b) Natureza do evento, como por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha, etc;

c) Data, hora e fuso horário, observando o previsto no item 6.1; e

d) Endereço IP (*Internet Protocol*), identificador do ativo de informação, coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento.

6.4 Os ativos de informação que não permitam os registros de eventos acima listados devem ser mapeados e documentados quanto ao tipo e formato de registros de auditoria que o sistema permita armazenar.

6.5 Devem-se acompanhar os sistemas e redes de comunicação de dados, registrando-se os eventos de segurança elencados abaixo, sem prejuízo de outros considerados relevantes:

a) Utilização de usuários, perfis e grupos privilegiados;

b) Inicialização, suspensão e reinicialização de serviços;

c) Acoplamento e desacoplamento de dispositivos de hardware, com especial atenção para mídias removíveis;

d) Modificações da lista de membros de grupos privilegiados;

e) Modificações de política de senhas, como por exemplo, tamanho, expiração, bloqueio automático após exceder determinado número de tentativas de autenticação, histórico; etc.

f) Acesso ou modificação de arquivos ou sistemas considerados críticos; e

g) Eventos obtidos de quaisquer mecanismos de segurança existentes.

6.6 Os servidores de hospedagem de página eletrônica, bem como todo e qualquer outro ativo de informação que assim o permita, devem ser configurados para armazenar registros históricos de eventos (*Logs*) em formato que permita a completa identificação dos fluxos de dados.

6.7 Os registros devem ser armazenados pelo período mínimo de 06 (seis) meses, sem prejuízo de outros prazos previstos em normativos específicos.

6.8 Recomenda-se que os ativos de informação sejam configurados de forma a armazenar seus registros de auditoria não apenas localmente, como também remotamente, por meio do uso de tecnologia aplicável.

7 DOS PROCEDIMENTOS PARA COLETA E PRESERVAÇÃO DAS EVIDÊNCIAS

7.1 O agente responsável pela ETIR, durante o processo de tratamento do incidente, e particularmente nos casos dos eventos previstos no item 5, deverá, sem prejuízo de outras ações, coletar e preservar:

a) As mídias de armazenamento dos dispositivos afetados; e

b) Todos os registros de eventos citados no item 6.

7.2 Nos casos em que seja inviável preservar as mídias de armazenamento mencionadas na alínea "a" do item 7.1, em razão da necessidade de pronto restabelecimento do serviço afetado, o agente responsável pela ETIR deverá coletar e armazenar cópia dos arquivos afetados pelo incidente, tais como: *Logs*, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original, bem como os "metadados" desses arquivos, como data, hora de criação e permissões.

7.3 O agente responsável pela ETIR deve fazer constar em relatório a impossibilidade de preservar as mídias afetadas e listar todos os procedimentos adotados.

7.4 As ações de restabelecimento do serviço não devem comprometer a coleta, e preservação da integridade das evidências.

7.5 Para a preservação dos arquivos coletados, deve-se:

a) Gerar um arquivo contendo a lista dos resumos criptográficos de todos os arquivos coletados;

b) Gravar os arquivos coletados, acompanhado do arquivo com a lista dos resumos criptográficos descrito na alínea anterior; e

c) Gerar o resumo criptográfico do arquivo citado na alínea "a" deste item.

7.6 Todo material coletado deverá ser lacrado e custodiado pelo agente responsável pela ETIR, o qual deve preencher Termo de Custódia dos Ativos de Informação relacionados ao Incidente de Segurança. O material coletado ficará à disposição da autoridade comunicada, a qual orientará quanto à sua destinação.

8 DA COMUNICAÇÃO ÀS AUTORIDADES COMPETENTES

8.1 Após a conclusão do processo de coleta e preservação das evidências do incidente, o responsável pela ETIR deverá elaborar Relatório de Comunicação de Incidente de Segurança em Redes Computacionais, descrevendo detalhadamente os eventos verificados.

8.1.1 O Relatório de Comunicação de Incidente de Segurança em Redes Computacionais deverá ser instruído com os seguintes elementos, sem detrimento a outras informações julgadas relevantes, devendo ser justificada a indisponibilidade de alguma informação:

a) O nome do responsável pela preservação dos dados do incidente, com informações de contato;

b) O nome do agente responsável pela ETIR, e informações de contato;

c) Órgão comunicante com sua localização e informações de contato;

d) Número de controle da ocorrência;

e) Relato sobre o incidente, descrevendo como ocorreu o fato, como foi detectado, os dados coletados e preservados, bem como outros dados considerados relevantes.

f) Descrição das atividades de tratamento e resposta ao incidente, bem como outras providências tomadas pela ETIR incluindo as ações de preservação, registrando-se a metodologia, caso aplicada, as ferramentas utilizadas e o local de armazenamento das informações preservadas;

g) O resumo criptográfico citado no item 7.5;

h) Termo de Custódia dos Ativos de Informação Relacionados ao Incidente de Segurança;

i) Número de lacre de material físico preservado, se houver; e

j) Justificativa sobre a inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados, nos termos do item 7.3.

8.1.2 O Relatório de Comunicação de Incidente de Segurança em Redes Computacionais deverá ser acondicionado em envelope lacrado e rubricado pelo agente responsável pela ETIR, protocolado e encaminhado formalmente à autoridade responsável pelo órgão ou entidade da APF.

8.1.3. A comunicação formal a que se refere o item 8.1.2 deverá apenas fazer menção de que se trata de comunicação de evento relacionado à segurança da informação, sem a descrição dos fatos.

8.2 Após receber a comunicação, a autoridade responsável pelo órgão ou entidade da APF deverá, de imediato, encaminhá-la formalmente à autoridade com atribuição para apurar os fatos. A

comunicação deverá ser acompanhada de envelope lacrado contendo o relatório mencionado no item 8.1.2.

8.2.1 Como no item 8.1.3, a comunicação de encaminhamento deverá informar que se trata de evento relacionado à SIC, sem a descrição dos fatos.

8.3 A critério do responsável pela ETIR e da autoridade responsável pelo órgão, os atos preparatórios e as tentativas também poderão ser comunicados na forma descrita nos itens anteriores.

8.4 A preservação da privacidade e sigilo dos dados custodiados deverá ser observada durante todo o processo de coleta das evidências do incidente de segurança em redes computacionais, na elaboração do relatório, bem como, quando do seu envio às autoridades competentes, conforme legislação vigente.

8.4.1 O Relatório de Comunicação de Incidentes de Segurança em Redes Computacionais (modelo exemplificado no anexo A) e o Termo de Custódia dos Ativos de Informação relacionados ao Incidente de Segurança (modelo exemplificado no anexo B) contêm informações sigilosas amparadas em hipóteses de sigilo previstas na legislação vigente.

8.4.2 Os órgãos e entidades da APF deverão adotar normas e procedimentos internos de tratamento das informações sigilosas que constam no Relatório de Comunicação de Incidente de Segurança em Redes Computacionais, e no Termo de Custódia dos Ativos de Informação Relacionados ao Incidente de Segurança.

9 DAS RESPONSABILIDADES

9.1 Cabe à Alta Administração do órgão ou entidade da APF aprovar as diretrizes gerais para cumprimento desta Norma observada, dentre outros, a Política de Segurança da Informação e Comunicações e a Gestão de Riscos de Segurança da Informação e Comunicações, bem como a sua missão e os seus objetivos estratégicos. Tais diretrizes, todavia, não poderão conter disposições que inviabilizem o desempenho dos procedimentos previstos nos itens 6, 7 e 8 desta Norma.

9.2 Cabe aos Gestores de Segurança da Informação e Comunicações coordenar a instituição, implementação e manutenção da infraestrutura necessária às ETIR, nos órgãos e entidades da APF, direta e indireta, conforme descrito no inciso V do art 5º da Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008.

9.3 Cabe ao Agente Responsável pela ETIR, para efeito desta Norma, o acompanhamento do processo de identificação e classificação de ativos de informação, o acompanhamento e registro

de eventos de segurança e a utilização de metodologia e ferramentas reconhecidas e recomendadas em referenciais técnicos quanto ao processo de coleta e preservação de evidências.

10 VIGÊNCIA

Esta Norma Complementar entra em vigor em 180 dias após a data de sua publicação.

11 ANEXOS

A – EXEMPLO DE MODELO DE RELATÓRIO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA EM REDES COMPUTACIONAIS

B – EXEMPLO DE MODELO DE TERMO DE CUSTÓDIA DOS ATIVOS DE INFORMAÇÃO RELACIONADOS AO INCIDENTE DE SEGURANÇA

ANEXO A – EXEMPLO DE MODELO DE 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: _____

RELATO SOBRE O INCIDENTE:

DESCREVA O INCIDENTE:

_____

_____

_____

_____

_____

_____

_____

_____

SE POSSÍVEL, DESCREVA A 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

ANEXO B – EXEMPLO DE MODELO DE TERMO DE CUSTÓDIA DOS ATIVOS DE INFORMAÇÃO RELACIONADOS AO INCIDENTE DE SEGURANÇA

DADOS GERAIS:

Nome do custodiante: Matrícula: Nome do Órgão/Entidade da APF: Cargo/Função: Endereço: Telefone: Endereço eletrônico:

MATERIAIS SOB CUSTÓDIA:

ITEM	TIPO	QTDE	DESCRIÇÃO	IDENTIF./LACRE

_____

Local e data

_____

Assinatura do Custodiante