Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008.

Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

O MINISTRO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, na condição de SECRETÁRIO-EXECUTIVO DO CONSELHO DE DEFESA NACIONAL, no uso de suas atribuições;

CONSIDERANDO:

o disposto no artigo 6º e parágrafo único do art. 16 da Lei nº 10.683, de 28 de maio de 2003;

o disposto no inciso IV do *caput* e inciso III do §1º do art. 1º e art. 8º do Anexo I do Decreto nº 5.772, de 08 de maio de 2006;

o disposto nos incisos I, VI, VII e XIII do artigo 4º do Decreto nº 3.505, de 13 de junho de 2000;

as informações tratadas no âmbito da Administração Pública Federal, direta e indireta, como ativos valiosos para a eficiente prestação dos serviços públicos;

o interesse do cidadão como beneficiário dos serviços prestados pelos órgãos e entidades da Administração Pública Federal, direta e indireta;

o dever do Estado de proteção das informações pessoais dos cidadãos;

a necessidade de incrementar a segurança das redes e bancos de dados governamentais; e

a necessidade de orientar a condução de políticas de segurança da informação e comunicações já existentes ou a serem implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

RESOLVE:

Art. 1º Aprovar orientações para Gestão de Segurança da Informação e Comunicações que deverão ser implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

Art. 2º Para fins desta Instrução Normativa, entende-se por:

I - Política de Segurança da Informação e Comunicações: documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte

administrativo suficientes à implementação da segurança da informação e comunicações;

II - Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

III - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

IV - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

V - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

VI - 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;

VII - Gestão de Segurança da Informação e Comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

VIII - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

IX - tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

Art. 3º Ao Gabinete de Segurança Institucional da Presidência da República - GSI, por intermédio do Departamento de Segurança da Informação e Comunicações - DSIC, compete:

I - planejar e coordenar as atividades de segurança da informação e comunicações na Administração Pública Federal, direta e indireta;

II - 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;

III - operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da Administração Pública Federal, direta e indireta, denominado CTIR.GOV;

IV - elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos em segurança da informação e comunicações;

V - orientar a condução da Política de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;

VI - receber e consolidar os resultados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta;

VII - propor programa orçamentário específico para as ações de segurança da informação e comunicações.

Art. 4º Ao Comitê Gestor de Segurança da Informação compete:

I - assessorar o GSI no aperfeiçoamento da Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta;

II - instituir grupos de trabalho para tratar de temas específicos relacionados à segurança da informação e comunicações.

Art. 5º Aos demais órgãos e entidades da Administração Pública Federal, direta e indireta, em seu âmbito de atuação, compete:

I - coordenar as ações de segurança da informação e comunicações; II - aplicar as ações corretivas e disciplinares cabíveis nos casos de quebra de segurança;

III - propor programa orçamentário específico para as ações de segurança da informação e comunicações;

IV - nomear Gestor de Segurança da Informação e Comunicações;

V - instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais;

VI - instituir Comitê de Segurança da Informação e Comunicações;

VII - aprovar Política de Segurança da Informação e Comunicações e demais normas de segurança da informação e comunicações;

VIII - remeter os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações para o GSI.

Parágrafo único. Para fins do disposto no *caput*, deverá ser observado o disposto no inciso II do art. 3º desta Instrução Normativa.

Art. 6º Ao Comitê de Segurança da Informação e Comunicações, de que trata o inciso VI do art. 5º, em seu âmbito de atuação, compete:

I - assessorar na implementação das ações de segurança da informação e comunicações;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações; III - propor alterações na Política de Segurança da Informação e Comunicações; e

IV - propor normas relativas à segurança da informação e comunicações.

Art. 7º Ao Gestor de Segurança da Informação e Comunicações, de que trata o inciso IV do art. 5º, no âmbito de suas atribuições, incumbe:

I - promover cultura de segurança da informação e comunicações;

II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III - propor recursos necessários às ações de segurança da informação e comunicações;

IV - coordenar o Comitê de Segurança da Informação e Comunicações e a equipe de tratamento e resposta a incidentes em redes computacionais;

V - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

VI - manter contato direto com o DSIC para o trato de assuntos relativos à segurança da informação e comunicações;

VII - propor normas relativas à segurança da informação e comunicações.

Art. 8º O cidadão, como principal cliente da Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta, poderá apresentar sugestões de melhorias ou denúncias de quebra de segurança que deverão ser averiguadas pelas autoridades.

Art. 9º Esta Instrução Normativa entra em vigor sessenta dias após sua publicação.

JORGE ARMANDO FELIX

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

ATIVIDADE DE NORMATIZAÇÃO

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

Artigo 6º da Lei nº 10.683, de 28 de maio de 2003.
Art. 8º do Anexo I do Decreto nº 5.772, de 8 de maio de 2006.
Decreto nº 3.505, de 13 de junho de 2000.
Art. 3º da IN nº 01 do Gabinete de Segurança Institucional, de 13 de Junho de 2008.

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 critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta.

2 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.

3 ELABORAÇÃO DAS NORMAS

Cabe a cada órgão e entidade da Administração Pública Federal, direta e indireta, em seu âmbito de atuação, aprovar as normas de segurança da informação e comunicações.

4 APRESENTAÇÃO DAS NORMAS

4.1 A critério da autoridade competente de cada órgão e entidade da Administração Pública Federal, direta e indireta, a Política de Segurança da Informação e Comunicações e demais normas de segurança da informação e comunicações poderão ser elaboradas conforme a seguinte formatação:

4.2 Folha-de-Rosto e Folha de Continuação das Normas

4.2.1 A Folha-de-rosto de cada norma complementar contendo os elementos que a identifiquem e explicitem o seu conteúdo, contemplando as seguintes informações:

a) **Indicação do órgão ou entidade** da Administração Pública Federal, direta e indireta;
b) **Número da Norma**: código estabelecido conforme detalhamento constante do subitem 4.6.1 desta Norma;
c) **Revisão**: número seqüencial da revisão, identificada por dois algarismos arábicos, sendo 00 a emissão original;
d) **Emissão**: dia, mês e ano de emissão da norma ou de sua revisão (exemplo: 22/JAN/00);
e) **Folha**: número da folha / total de folhas (exemplo: 1/13);
f) **Título da Norma**: expressão identificadora do conteúdo da norma, de forma concisa, precisa e inequívoca; digitado com a fonte “Times New Roman” tamanho 14 em negrito;
g) **Origem**: unidade responsável pela atividade normativa;
h) **Referência Normativa**: documentos normativos e respectivas datas de aprovação, se houver;
i) **Campo de Aplicação**: unidades onde se aplica a norma e/ou áreas envolvidas com a execução e com o acompanhamento do assunto nela tratado;
j) **Sumário**: lista dos itens constantes da norma, que permite uma visão global e facilita a sua consulta;

k) **Informações adicionais** esclarecimentos sobre a edição ou revisão da norma, especialmente quanto a substituições e cancelamentos de normas anteriores; e
l) **Aprovação**: assinatura da norma pela autoridade competente.

4.2.2 As folhas de continuação da norma são identificadas, na sua parte superior direita, pelo conjunto de informações contendo: número da norma complementar, revisão, emissão e folha.

4.2.3 O modelo da folha-de-rosto das normas constitui o **Anexo A** desta Norma.

4.3 Conteúdo das Normas

4.3.1 As normas complementares podem conter uma estrutura básica, compostas dos seguintes itens:
a) **Objetivo:** definir o escopo da norma e os aspectos por ela abrangidos;
b) **Procedimentos:** passos estabelecidos, em seqüência lógica, correspondentes ao assunto tratado, abrangendo todas as tarefas envolvidas no processo;
c) **Disposições Gerais:** informações adicionais julgadas necessárias, especialmente com relação a esclarecimento de eventuais dúvidas e casos omissos;
d) **Vigência**: data em que a norma entra em vigor; e
e) **Anexos**: formulários, fluxogramas e dados adicionais, necessários à execução da atividade constante da norma ou que facilitem a sua compreensão ou uso.

4.3.2 Os procedimentos podem estar divididos em vários itens, observadas as orientações constantes do item 4.5.4 desta Norma.

4.3.3 Sempre que uma sigla é citada pela primeira vez em uma norma, ela deve ser colocada entre parênteses, logo após o nome por extenso. O uso da sigla só se justifica quando é usado repetidamente na norma.

4.3.4 Serão grafadas por extenso quaisquer referências, feitas no texto, a números e percentuais (trinta, dez, treze, dois vírgula quinze por cento, etc), exceto nos casos em que houver prejuízo para compreensão do texto.

4.3.5 Valores monetários devem ser expressos em algarismos arábicos, seguidos da indicação, por extenso, entre parênteses.

4.4 Conteúdo das Normas

4.4.1 A redação deve ter estilo próprio, lingüisticamente correta, sem preocupações literárias e, tanto quanto possível, uniforme. A qualidade essencial é a clareza do texto, que deve ser facilmente compreensível por pessoas que não tenham participado na elaboração da norma.

4.4.2 Para maior clareza e objetividade deve-se:
a) construir as frases em ordem direta (sujeito, verbo, complementos);
b) utilizar frases curtas, para facilitar o entendimento e evitar duplo sentido;
c) usar, preferencialmente, o substantivo em lugar do pronome, mesmo com o prejuízo da elegância da frase;
d) utilizar termos técnicos já definidos em terminologia existente;

e) usar, preferencialmente, o presente do indicativo, salvo quando a regência gramatical exigir o uso de outros tempos ou modos;
f) utilizar o verbo no infinitivo nas descrições de etapas (exemplos: elaborar, emitir, aprovar); e
g) evitar detalhes excessivos e desnecessários que inibam a criatividade.

4.4.3 As aspas devem ser utilizadas para:
a) dar ênfase a um determinado termo;
b) indicar termo de língua estrangeira; e
c) indicar expressões de linguagem, comumente usadas no meio da especialidade, as quais, todavia, ainda não foram incorporadas ao vernáculo.

4.5 Estrutura do Texto

4.5.1 O texto pode ser subdividido em:
a) itens e subitens; e
b) alíneas e subalíneas.

4.5.2 Os itens podem ser divididos em até três subitens, numerados progressivamente em algarismos arábicos, conforme exemplo apresentado no **Anexo B** desta Norma.

4.5.3 Os títulos dos itens devem ser escritos em letras maiúsculas e em negrito, a fim de facilitar a sua identificação e localização. A escolha dos títulos dos itens deve ser feita de maneira criteriosa, de forma a permitir reconhecer a seqüência lógica de estruturação da norma. Para facilitar essa estruturação, deve-se definir a lista de todos os aspectos a serem incluídos, antes do início de sua redação.

4.5.4 A matéria do item deve ser apresentada em um único parágrafo, podendo, entretanto, existir uma ou mais frases. Caso o assunto seja extenso, o item deve ser dividido em dois ou mais subitens.

7.1 Ação Preventiva	***INCORRETO***
7.1.1 A organização deve...	***Só deveria existir 7.1.1 se existisse o 7.1.2***
7.2 Gestão de Recursos	***CORRETO***
7.2.1 Provisão de Recursos...	***Existem 7.2.1 e 7.2.2***
7.2.2 Treinamento, conscientização e....	

4.5.5 A numeração do item deve ficar junto à margem esquerda da página. Após o último número não se deve colocar ponto, parênteses ou hífen. Entre a numeração e a primeira letra seguinte (seja título ou não) deve ser dado um espaçamento correspondente a dois espaços.

4.5.6 Sempre que o título de um item ocupar mais de uma linha, a segunda e as demais linhas devem ser alinhadas com a primeira letra do título.

4.5.7 Em algumas situações os subitens podem ter títulos. Nestes casos, todas as palavras são escritas com apenas a primeira letra em maiúsculo.

4.5.8 A apresentação do assunto de um subitem na forma de alíneas, ordenadas alfabeticamente, traz clareza e rapidez na compreensão e visualização das idéias. Na identificação das alíneas deve ser usado o alfabeto completo, incluindo-se as letras “k”, “y” e “w”.

4.5.9 A disposição gráfica das alíneas obedece às seguintes regras:

a) dentro da alínea somente devem ser usadas vírgulas, isto é, a alínea deve ter uma única frase;
b) as alíneas devem ser ordenadas por letras minúsculas, seguidas de parênteses, sem ponto ou hífen após os parênteses;
c) nas alíneas de subitens:
   - alinhamento das suas letras indicativas deve possuir recuo constante de dez espaços, correspondente a um TAB, em relação à margem esquerda do texto principal;
   - seu texto, quando ocupar mais de uma linha, deve ser alinhado com a primeira letra da alínea;
d) o texto da alínea deve terminar por ponto-e-vírgula, exceto:
   - nos casos em que são seguidas de subalíneas, quando deve terminar por dois-pontos;
   - na última alínea, onde deve terminar por ponto; e
e) nas seqüências de alíneas e subalíneas, o penúltimo elemento é pontuado com ponto e vírgula seguido da conjunção “e”, quando de caráter cumulativo, ou da conjunção “ou” , se a seqüência for disjuntiva.

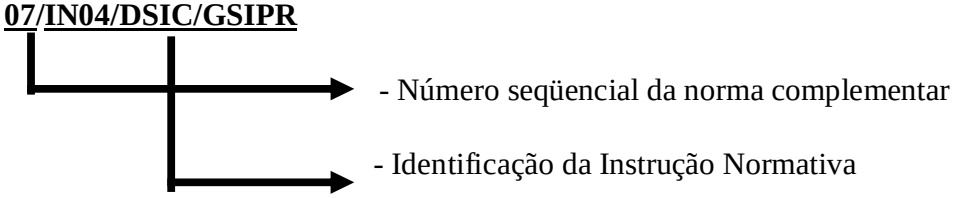
4.5.10 As subalíneas devem ser utilizadas para subdividir o assunto de uma alínea, tornando mais clara a sua compreensão. A subalínea deve ser indicada apenas por um hífen, sem indicativo de número ou letra.

4.5.11 O texto deve ser digitado em editor de texto, utilizando a fonte “Times New Roman”, tamanho 12.

4.5.12 A apresentação do texto com os recuos de seus elementos em relação às margens é apresentado no **Anexo C** desta Norma.

4.6 Numeração das Normas

4.6.1 As normas complementares podem ser numeradas conforme a seguinte ordem de formação, exemplificada a seguir:



4.6.2 Os anexos são identificados por letra maiúscula, seqüencialmente pela ordem em que aparecem no texto da norma. A citação dos anexos no texto será em negrito.

5 ATUALIZAÇÃO DAS NORMAS

5.1 Uma norma pode ser atualizada ou cancelada pela ocorrência de alguma das seguintes situações:

a) alteração dos procedimentos vigentes ou adoção de novos;
b) estabelecimento de novos dispositivos legais ou regulamentares, bem como reformulação dos existentes;
c) acolhimento de sugestões dos usuários, visando ao seu aperfeiçoamento; ou
d) encerramento de atividades.

5.2 Os procedimentos para aprovação e divulgação das normas alteradas seguem a mesma tramitação de uma norma nova.

6 DISPOSIÇÕES GERAIS

Os casos omissos e as dúvidas com relação a esta Norma serão submetidos ao Diretor do DSIC.

7 VIGÊNCIA

Esta Norma entra em vigor na data de sua publicação.

8 ANEXOS

A - Folha-de-rosto e folha de continuação das normas
B - Exemplo de numeração de itens
C - Apresentação da estrutura do texto com os recuos dos seus elementos em relação às margens

Anexo A

FOLHA-DE-ROSTO E FOLHA DE CONTINUAÇÃO DA NORMA

Número da Norma Complementar	Revisão	Emissão	Folha

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

TÍTULO DA NORMA

ORIGEM

REFERENCIA NORMATIVA

CAMPO DE APLICAÇAO

SUMARIO

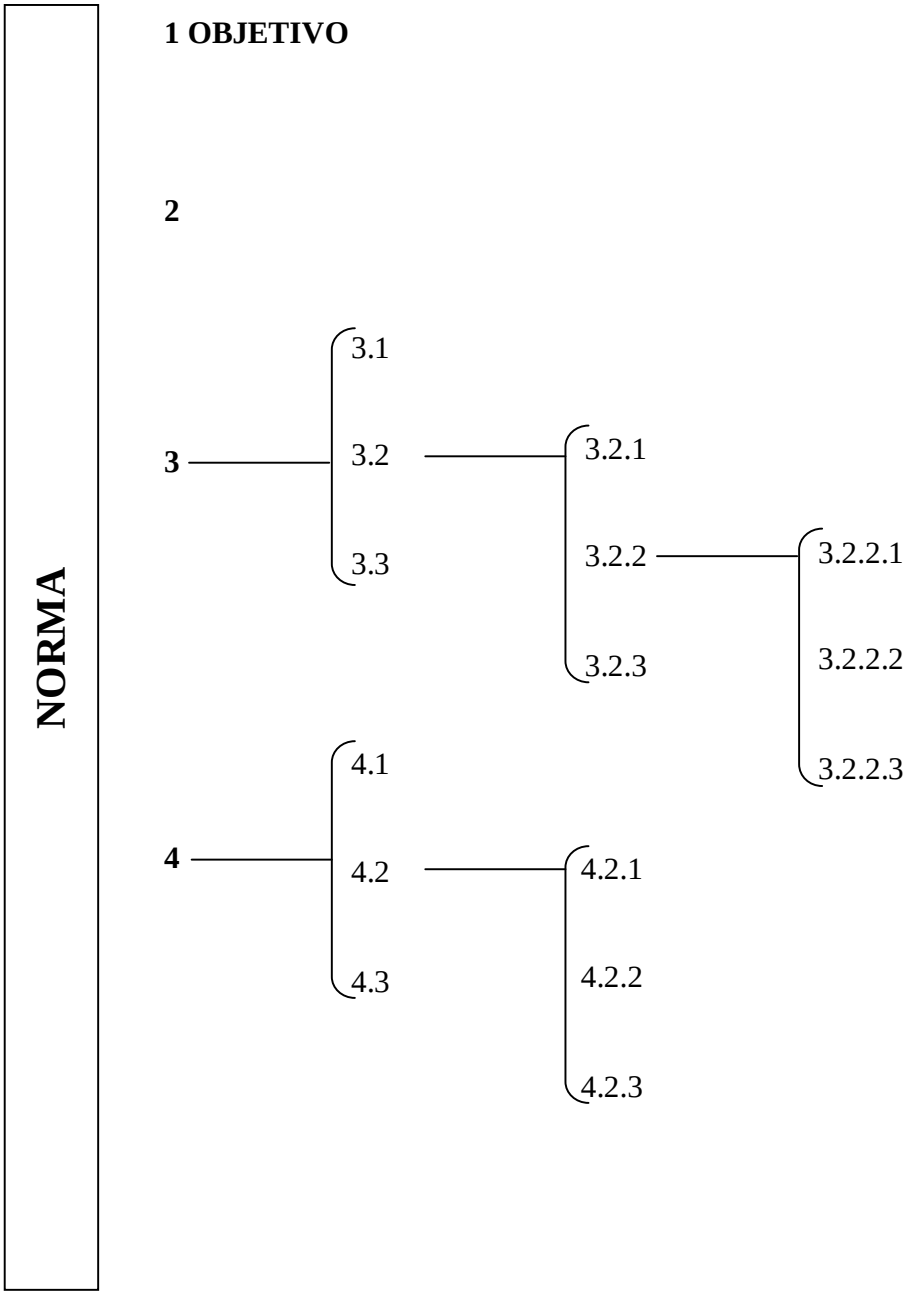
INFORMAÇOES ADICIONAIS

APROVAÇAO

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

Anexo B

EXEMPLO DE NUMERAÇÃO DE ITENS



Anexo C
APRESENTAÇÃO DA ESTRUTURA DO TEXTO COM OS RECUOS DOS SEUS ELEMENTOS EM RELAÇÃO ÀS MARGENS

Número da Norma Complementar	Revisão	Emissão	Folha

5 XXXX

5.1

5.1 .1

a)

b)

-

-

5.2

5.2 .1

5.2 .1.1

5.2 .1.2

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

METODOLOGIA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

Instrução Normativa GSI nº 1, de 13 de junho de 2008.
ABNT NBR ISO/IEC 27001:2006.

CAMPO DE APLICAÇÃO

Esta Norma 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

Definir a metodologia de gestão de segurança da informação e comunicações utilizada pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

2 METODOLOGIA

2.1 A metodologia de gestão de segurança da informação e comunicações baseia-se no processo de melhoria contínua, denominado ciclo **"PDCA"** *(Plan-Do-Check-Act)*, estabelecido pela norma ABNT NBR ISO/IEC 27001:2006.

2.2 A escolha desta metodologia levou em consideração três critérios:

a) Simplicidade do modelo;
b) Compatibilidade com a cultura de gestão de segurança da informação em uso nas organizações públicas e privadas brasileiras; e
c) Coerência com as práticas de qualidade e gestão adotadas em órgãos públicos brasileiros.

3 CICLO DA METODOLOGIA

3.1 ("**Plan – P**") Planejar - É a fase do ciclo na qual o Gestor de Segurança da Informação e Comunicações planejará as ações de segurança da informação e comunicações que serão implementadas, considerando os requisitos ou pressupostos estabelecidos pelo planejamento organizacional, bem como as diretrizes expedidas pela autoridade decisória de seu órgão ou entidade. Para planejar é necessário:

3.1.1 Definir o escopo e os limites onde serão desenvolvidas as ações de segurança da informação e comunicações;

3.1.2 Definir os objetivos a serem alcançados com a implementação das ações de segurança da informação e comunicações, considerando as expectativas ou diretrizes formuladas pela autoridade decisória de seu órgão ou entidade;

3.1.3 Definir a abordagem de gestão de riscos de seu órgão ou entidade, sendo necessário:

a) definir uma metodologia de gestão de riscos que seja adequada ao escopo, limites e objetivos estabelecidos;
b) identificar os níveis de riscos aceitáveis e os critérios para sua aceitação, considerando decisões superiores e o planejamento estratégico do órgão ou entidade;

3.1.4 Identificar os riscos, sendo necessário:

a) Identificar os ativos e seus responsáveis dentro do escopo onde serão desenvolvidas as ações de segurança da informação e comunicações;
b) Identificar as vulnerabilidades destes ativos;

c) Identificar os impactos que perdas de disponibilidade, integridade, confidencialidade e autenticidade podem causar nestes ativos;

3.1.5 Analisar os riscos, sendo necessário:

a) identificar os impactos para a missão do órgão ou entidade que podem resultar de falhas de segurança, levando em consideração as conseqüências de uma perda de disponibilidade, integridade, confidencialidade ou autenticidade destes ativos;
b) identificar a probabilidade real de ocorrência de falhas de segurança, considerando as vulnerabilidades prevalecentes, os impactos associados a estes ativos e as ações de segurança da informação e comunicações atualmente implementadas no órgão ou entidade;
c) estimar os níveis de riscos;
d) determinar se os riscos são aceitáveis ou se requerem tratamento utilizando os critérios para aceitação de riscos estabelecidos em 3.1.3;

3.1.6 Identificar as opções para o tratamento de riscos, considerando a possibilidade de:

a) aplicar ações de segurança da informação e comunicações além das que já estão sendo executadas;
b) aceitar os riscos de forma consciente e objetiva, desde que satisfaçam o planejamento organizacional, bem como a diretrizes expedidas pela autoridade decisória de seu órgão ou entidade, bem como aos critérios de aceitação de riscos estabelecidos em 3.1.3;
c) evitar riscos;
d) transferir os riscos a outras partes, por exemplo, seguradoras ou terceirizados;

3.1.7 Selecionar as ações de segurança da informação e comunicações consideradas necessárias para o tratamento de riscos. (Alguns exemplos de ações de segurança da informação e comunicações são: Política de Segurança da Informação e Comunicações, infra-estrutura de segurança da informação e comunicações, tratamento da informação, segurança em recursos humanos, segurança física, segurança lógica, controle de acesso, segurança de sistemas, tratamento de incidentes, gesta de continuidade, conformidade, auditoria interna, além de outras que serão exploradas em outras normas complementares);

3.1.8 Obter aprovação da autoridade decisória de seu órgão ou entidade quanto aos riscos residuais propostos;

3.1.9 Obter autorização da autoridade decisória de seu órgão ou entidade para implementar as ações de segurança da informação e comunicações selecionadas, mediante uma Declaração de Aplicabilidade, incluindo o seguinte:

a) Os objetivos e os recursos necessários para cada ação de segurança da informação e comunicações selecionada e as razões para sua seleção;
b) Os objetivos de cada ação de segurança da informação e comunicações que já foram implementadas em seu órgão ou entidade;
c) Um resumo das decisões relativas à gestão de riscos; e

d) Justificativas de possíveis exclusões de ações de segurança da informação e comunicações sugeridas pelo Gestor de Segurança da Informação e Comunicações e não autorizadas pela autoridade decisória de seu órgão ou entidade.

3.2 **("Do – D")** Fazer - É a fase do ciclo na qual o Gestor de Segurança da Informação e Comunicações implementará as ações de segurança da informação e comunicações definidas na fase anterior. Para fazer é necessário:

3.2.1 Formular um plano de metas para cada objetivo das ações de segurança da informação e comunicações aprovadas na fase do planejamento em ordem de prioridade, incluindo a atribuição de responsabilidades, os prazos para execução, e os custos estimados;

3.2.2 Obter autorização da autoridade decisória de seu órgão ou entidade para implementar o plano de metas com a garantia de alocação dos recursos planejados;

3.2.3 Implementar o plano de metas para atender as ações de segurança da informação e comunicações aprovadas;

3.2.4 Definir como medir a eficácia das ações de segurança da informação e comunicações, estabelecendo indicadores mensuráveis para as metas aprovadas;

3.2.5 Implementar programas de conscientização e treinamento, sendo necessário:

a) assegurar que todo pessoal que tem responsabilidades atribuídas no plano de metas receba o treinamento adequado para desempenhar suas tarefas;
b) manter registros sobre habilidades, experiências e qualificações do efetivo do órgão ou entidade relativos à segurança da informação e comunicações;
c) assegurar que todo efetivo do órgão ou entidade esteja consciente da relevância e importância da segurança da informação e comunicações em suas atividades e como cada pessoa pode contribuir para o alcance dos objetivos das ações de segurança da informação e comunicações;

3.2.6 Gerenciar a execução das ações de segurança da informação e comunicações;

3.2.7 Gerenciar os recursos empenhados para o desenvolvimento das ações de segurança da informação e comunicações; e

3.2.8 Implementar procedimentos capazes de permitir a pronta detecção de incidentes de segurança da informação e comunicações, bem como a resposta a incidentes de segurança da informação e comunicações.

3.3 **("Check – C")** Checar - É a fase do ciclo na qual o Gestor de Segurança da Informação e Comunicações avaliará as ações de segurança da informação e comunicações implementadas na fase anterior. Para checar é necessário:

3.3.1 Executar procedimentos de avaliação e análise crítica, a fim de:

a) detectar erros nos resultados de processamento;
b) identificar incidentes de segurança da informação e comunicações;
c) determinar se as ações de segurança da informação e comunicações delegadas a pessoas ou implementadas por meio de tecnologia da informação e comunicações estão sendo executadas conforme planejado;
d) determinar a eficácia das ações de segurança da informação e comunicações adotadas, mediante o uso de indicadores;

3.3.2 Realizar análises críticas regulares, a intervalos planejados de pelo menos uma vez por ano;

3.3.3 Verificar se os requisitos ou pressupostos estabelecidos pelo planejamento organizacional, bem como as diretrizes expedidas pela autoridade decisória de seu órgão ou entidade foram atendidos;

3.3.4 Atualizar a avaliação/análise de riscos a intervalos planejados de pelo menos uma vez por ano;

3.3.5 Conduzir auditoria interna, também denominada auditoria de primeira parte, das ações de segurança da informação e comunicações a intervalos planejados de pelo menos uma vez ao ano;

3.3.6 Atualizar os planos de segurança da informação e comunicações, considerando os resultados da avaliação e análise de crítica; e

3.3.7 Registrar e levar ao conhecimento da autoridade superior os possíveis impactos na eficácia da missão de seu órgão ou entidade.

3.4 **("Act – A")** Agir - É a fase do ciclo na qual o Gestor de Segurança da Informação e Comunicações aperfeiçoará as ações de segurança da informação e comunicações, baseando-se no monitoramento realizado na fase anterior. Para aperfeiçoar e promover a melhoria contínua é necessário:

3.4.1 Propor à autoridade decisória de seu órgão ou entidade a necessidade de implementar as melhorias identificadas;

3.4.2 Executar as ações corretivas ou preventivas de acordo com a identificação de não conformidade real ou potencial;

3.4.3 Comunicar as melhorias à autoridade decisória de seu órgão ou entidade; e

3.4.4 Assegurar-se de que as melhorias atinjam os objetivos pretendidos.

4 CONSIDERAÇÕES FINAIS

A metodologia apresentada nesta norma deve ser complementar aos primeiros processos de Gestão de Segurança da Informação e Comunicações, previstos na IN 01 GSI, de 13 de junho de 2008, a serem implementados pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

5 VIGÊNCIA DA NORMA

Esta Norma entra em vigor na data de sua publicação.

Número da Norma Complementar	Revisão	Emissão	Folha
03/IN01/DSIC/GSIPR	01	10/Jun/09	1/5

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

DIRETRIZES PARA ELABORAÇÃO DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NOS ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA LEGAL E NORMATIVA

Art. 6º da Lei nº 10.683, de 28 de maio de 2003.
Art. 8º do Anexo I do Decreto nº 5.772, de 8 de maio de 2006.
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.
NBR ISO/IEC 27002:2007.
NBR ISO/IEC 27005:2008.
Decreto nº 1048, de 21 de janeiro de 1994.
Decreto de 18 de outubro de 2000 - Governo Eletrônico.
Decreto nº 4553, de 27 de dezembro de 2002.
Art 5º Inciso III da Instrução Normativa nº 04 da Secretaria de Logística e Tecnologia da Informação/MPOG, de 19 de maio de 2008.
e-PING – Padrões de Interoperabilidade de Governo Eletrônico, de 16 de dezembro de 2008

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, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações (POSIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.

2 CONSIDERAÇÕES INICIAIS

2.1 A Política de Segurança da Informação e Comunicações declara o comprometimento da alta direção organizacional com vistas a prover diretrizes estratégicas, responsabilidades, competências e o apoio para implementar a gestão de segurança da informação e comunicações nos órgãos ou entidades da Administração Pública Federal, direta e indireta;

2.2 As diretrizes constantes na Política de Segurança da Informação e Comunicações no âmbito do órgão ou entidade visam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

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 são estabelecidos os seguintes conceitos e definições:

4.1 **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 do órgão ou entidade da APF;

4.2 **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR)**: grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;

4.3 **Gestor de Segurança da Informação e Comunicações**: é responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF;

4.4 **Política de Segurança da Informação e Comunicações (POSIC)**: documento aprovado pela autoridade responsável do órgão ou entidade da APF, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;

4.5 **Quebra de Segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.

5 ELABORAÇÃO DA POSIC

5.1 Recomenda-se que para a elaboração da POSIC seja instituído um Grupo de Trabalho constituído por representantes dos diferentes setores do órgão ou entidade da APF, como por exemplo: segurança patrimonial, tecnologia da informação, recursos humanos, jurídico, financeiro e planejamento;

5.2 A elaboração da POSIC deve levar em consideração a natureza e finalidade do órgão ou entidade da APF, alinhando-se sempre que possível à sua missão e ao planejamento estratégico;

5.3 Recomenda-se que na elaboração da POSIC sejam incluídos os seguintes itens:

5.3.1 **Escopo**: neste item recomenda-se descrever o objetivo e abrangência da Política de Segurança da Informação e Comunicações, definindo o limite no qual as ações de segurança da informação e comunicações serão desenvolvidas no órgão ou entidade da APF;

5.3.2 **Conceitos e definições**: neste item recomenda-se relacionar todos os conceitos e suas definições a serem utilizados na Política de Segurança da Informação e Comunicações do órgão ou entidade da APF que possam gerar dificuldades de interpretações ou significados ambíguos;

5.3.3 **Referências legais e normativas**: neste item recomenda-se relacionar as referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação e Comunicações do órgão ou entidade da APF;

5.3.4 **Princípios**: neste item recomenda-se relacionar os princípios que regem a segurança da informação e comunicações no órgão ou entidade da APF;

5.3.5 **Diretrizes Gerais**: neste item recomenda-se estabelecer diretrizes sobre, no mínimo, os seguintes temas, considerando as Normas específicas vigentes no ordenamento jurídico:

a) Tratamento da Informação;
b) Tratamento de Incidentes de Rede;
c) Gestão de Risco;
d) Gestão de Continuidade;
e) Auditoria e Conformidade;
f) Controles de Acesso;
g) Uso de e-mail; e
h) Acesso a Internet.

5.3.6 **Penalidades**: neste item identificam-se as conseqüências e penalidades para os casos de violação da Política de Segurança da Informação e Comunicações ou de quebra de segurança, devendo ser proposto um termo de responsabilidade;

5.3.7 **Competências e Responsabilidades**: neste item recomendam-se os seguintes procedimentos:

5.3.7.1 Definir a estrutura para a Gestão da Segurança da Informação e Comunicações;

5.3.7.2 Instituir o Gestor de Segurança da Informação e Comunicações do órgão ou entidade da APF, dentre servidores públicos civis ou militares, conforme o caso, com as seguintes responsabilidades:

a) Promover cultura de segurança da informação e comunicações;
b) Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
c) Propor recursos necessários às ações de segurança da informação e comunicações;
d) Coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
e) Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
f) Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações;
g) Propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito do órgão ou entidade da APF.

5.3.7.3 Instituir o Comitê de Segurança da Informação e Comunicações do órgão ou entidade da APF com as seguintes responsabilidades:

a) Assessorar na implementação das ações de segurança da informação e comunicações no órgão ou entidade da APF;
b) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações; e
c) Propor Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema.

5.3.7.4 Instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do órgão ou entidade da APF.

5.3.8 **Atualização**: neste item recomenda-se estabelecer a periodicidade da revisão da Política de Segurança da Informação e Comunicações ou dos instrumentos normativos gerados a partir da própria POSIC.

5.4 A POSIC precisa ser objetiva, simples, de fácil leitura e entendimento;

5.5 A POSIC poderá ser complementada por Normas e Procedimentos que a referenciem.

6 INSTITUCIONALIZAÇÃO DA POSIC

Para a institucionalização da POSIC no órgão ou entidade da APF, são recomendadas as seguintes ações:

6.1 Implementar a POSIC através da formalização e da aprovação por parte da autoridade máxima responsável pelo órgão ou entidade da APF, demonstrando a todos os servidores e usuários o seu comprometimento;

6.2 Garantir a provisão dos recursos necessários para a implementação da POSIC por parte do órgão ou entidade da APF;

6.3 Promover no órgão ou entidade da APF, a cultura de segurança da informação e comunicações, por meio de atividades de sensibilização, conscientização, capacitação e especialização.

7 DIVULGAÇÃO DA POSIC

A POSIC e suas atualizações deverão ser divulgadas a todos os servidores, usuários, prestadores de serviço, contratados e terceirizados que habitualmente trabalham no órgão ou entidade da APF.

8 ATUALIZAÇÃO DA POSIC

Todos os instrumentos normativos gerados a partir da POSIC, incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 03(três) anos.

9 VIGÊNCIA

Esta Norma entra em vigor na data de sua publicação.

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

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES – GRSIC

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 Anexo I do Decreto nº 5.772, de 8 de maio de 2006.
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.
Norma Complementar 01/DSIC/GSIPR de 13 de outubro de 2008.
Norma Complementar 02/DSIC/GSIPR de 13 de outubro de 2008.
ABNT NBR ISO/IEC 27001:2006.
ABNT NBR ISO/IEC 27005:2008.

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 processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF.

2 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.

3 CONCEITOS E DEFINIÇÕES

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

3.1 **Ameaça** – conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

3.2 **Análise de riscos** – uso sistemático de informações para identificar fontes e estimar o risco;

3.3 **Análise/avaliação de riscos** – processo completo de análise e avaliação de riscos;

3.4 **Ativos de Informação** – os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

3.5 **Avaliação de riscos** – processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

3.6 **Comunicação do risco** – troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas;

3.7 **Estimativa de riscos** – processo utilizado para atribuir valores à probabilidade e consequências de um risco;

3.8 **Evitar risco** – uma forma de tratamento de risco na qual a alta administração decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco;

3.9 **Gestão de Riscos de Segurança da Informação e Comunicações** – conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

3.10 **Identificação de riscos** – processo para localizar, listar e caracterizar elementos do risco;

3.11 **Reduzir risco** – uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco;

3.12 **Reter risco** – uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado;

3.13 **Riscos de Segurança da Informação e Comunicações** – potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

3.14 **Transferir risco** – uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;

3.15 **Tratamento dos riscos** – processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

3.16 **Vulnerabilidade** – conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

4 PRINCÍPIOS E DIRETRIZES

4.1 As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC deverão considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do órgão ou entidade da Administração Pública Federal, direta e indireta – APF, além de estarem alinhadas à respectiva Política de Segurança da Informação e Comunicações do órgão ou entidade;

4.2 O processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC deve ser contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações;

4.3 O processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC deve estar alinhado ao modelo denominado PDCA (*Plan-Do-Check-Act*), conforme definido na Norma Complementar nº 02/DSIC/GSIPR, publicada no Diário Oficial da União nº 199, Seção 1, de 14 de outubro de 2008, de modo a fomentar a sua melhoria contínua;

4.4 A Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC deverá produzir subsídios para suportar o Sistema de Gestão de Segurança da Informação e Comunicações e a Gestão de Continuidade de Negócios.

5 PROCEDIMENTOS

Nos itens abaixo será apresentada uma abordagem sistemática do processo Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC, com o objetivo de manter os riscos em níveis aceitáveis. Esse processo é composto pelas etapas de definições preliminares, análise/avaliação dos riscos, plano de tratamento dos riscos, aceitação dos riscos, implementação do plano de tratamento dos riscos, monitoração e análise crítica, melhoria do processo de Gestão de Riscos de Segurança da Informação e Comunicações e comunicação do risco, conforme apresentado no **Anexo A** desta Norma.

5.1 **Definições preliminares:** nesta fase, deve-se realizar uma análise da organização visando estruturar o processo de gestão de riscos de segurança da informação e comunicações, sendo consideradas as características do órgão ou entidade e as restrições a que estão sujeitas. Esta análise inicial permite que os critérios e o enfoque da Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC sejam os mais apropriados para o órgão, apoiando-o na definição do escopo e na adoção de uma metodologia.

5.1.1 Definir o escopo de aplicação da Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC a fim de delimitar o âmbito de atuação. Esse escopo pode abranger o órgão ou entidade como um todo, um segmento, um processo, um sistema, um recurso ou um ativo de informação;

5.1.2 Adotar uma metodologia de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC que atenda aos objetivos, diretrizes gerais e o escopo definido contemplando, no mínimo, os critérios de avaliação e de aceitação do risco.

5.2 **Análise/avaliação dos riscos:** nesta fase, inicialmente serão identificados os riscos, considerando as ameaças e as vulnerabilidades associadas aos ativos de informação para, em seguida, serem estimados os níveis de riscos de modo que eles sejam avaliados e priorizados.

5.2.1 Identificar os ativos e seus respectivos responsáveis dentro do escopo estabelecido;

5.2.2 Identificar os riscos associados ao escopo definido, considerando:

a) as ameaças envolvidas;
b) as vulnerabilidades existentes nos ativos de informação;
c) as ações de Segurança da Informação e Comunicações – SIC já adotadas.

5.2.3 Estimar os riscos levantados, considerando os valores ou níveis para a probabilidade e para a consequência do risco associados à perda de disponibilidade, integridade, confidencialidade e autenticidade nos ativos considerados;

5.2.4 Avaliar os riscos, determinando se são aceitáveis ou se requerem tratamento, comparando a estimativa de riscos com os critérios estabelecidos no item 5.1.2;

5.2.5 Relacionar os riscos que requeiram tratamento, priorizando-os de acordo com os critérios estabelecidos pelo órgão ou entidade.

5.3 **Plano de Tratamento dos Riscos**

5.3.1 Determinar as formas de tratamento dos riscos, considerando as opções de reduzir, evitar, transferir ou reter o risco, observando:

a) a eficácia das ações de Segurança da Informação e Comunicações – SIC já existentes;
b) as restrições organizacionais, técnicas e estruturais;
c) os requisitos legais;
d) a análise custo/ benefício.

5.3.2 Formular um plano para o tratamento dos riscos, relacionando, no mínimo, as ações de Segurança da Informação e Comunicações – SIC, responsáveis, prioridades e prazos de execução necessários à sua implantação.

5.4 **Aceitação do Risco:** verificar os resultados do processo executado, considerando o plano de tratamento, aceitando-os ou submetendo-os à nova avaliação.

5.5 **Implementação do Plano de Tratamento dos Riscos:** executar as ações de Segurança da Informação e Comunicações – SIC incluídas no Plano de Tratamento dos Riscos aprovado.

5.6 **Monitoração e análise crítica:** detectar possíveis falhas nos resultados, monitorar os riscos, as ações de Segurança da Informação e Comunicações – SIC e verificar a eficácia do processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC.

5.6.1 Do processo de gestão: monitorar e analisar criticamente o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC de forma a mantê-lo alinhado às diretrizes gerais estabelecidas e às necessidades do órgão ou entidade;

5.6.2 Do risco: manter os riscos monitorados e analisados criticamente, a fim de verificar regularmente, no mínimo, as seguintes mudanças:

a) nos critérios de avaliação e aceitação dos riscos;
b) no ambiente;
c) nos ativos de informação;
d) nas ações de Segurança da Informação e Comunicações – SIC;
e) nos fatores do risco (ameaça, vulnerabilidade, probabilidade e impacto).

5.7 **Melhoria do Processo de GRSIC**

5.7.1 Propor à autoridade decisória do órgão ou entidade a necessidade de implementar as melhorias identificadas durante a fase de monitoramento e análise crítica;

5.7.2 Executar as ações corretivas ou preventivas aprovadas;

5.7.3 Assegurar que as melhorias atinjam os objetivos pretendidos.

5.8 **Comunicação do Risco:** manter as instâncias superiores informadas a respeito de todas as fases da gestão de risco, compartilhando as informações entre o tomador da decisão e as demais partes envolvidas e interessadas.

6 RESPONSABILIDADES

6.1 Cabe à Alta Administração do órgão ou entidade da Administração Pública Federal, direta e indireta – APF aprovar as diretrizes gerais e o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC observada, dentre outras, a respectiva Política de Segurança da Informação e Comunicações;

6.2 Os Gestores de Segurança da Informação e Comunicações, no âmbito de suas atribuições, são responsáveis pela coordenação da Gestão de Riscos de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

6.3 De acordo com as necessidades de cada órgão ou entidade, os Gestores de Segurança da Informação e Comunicações poderão indicar responsáveis pelo gerenciamento de atividades, a quem serão conferidas, no mínimo, as seguintes atribuições:

6.3.1 análise/avaliação e tratamento dos riscos;

6.3.2 elaboração sistemática de relatórios para os Gestores de Segurança da Informação e Comunicações, em cujo conteúdo constará a análise quanto à aceitação dos resultados obtidos, e consequente proposição de ajustes e de medidas preventivas e proativas à Alta Administração.

7 VIGÊNCIA

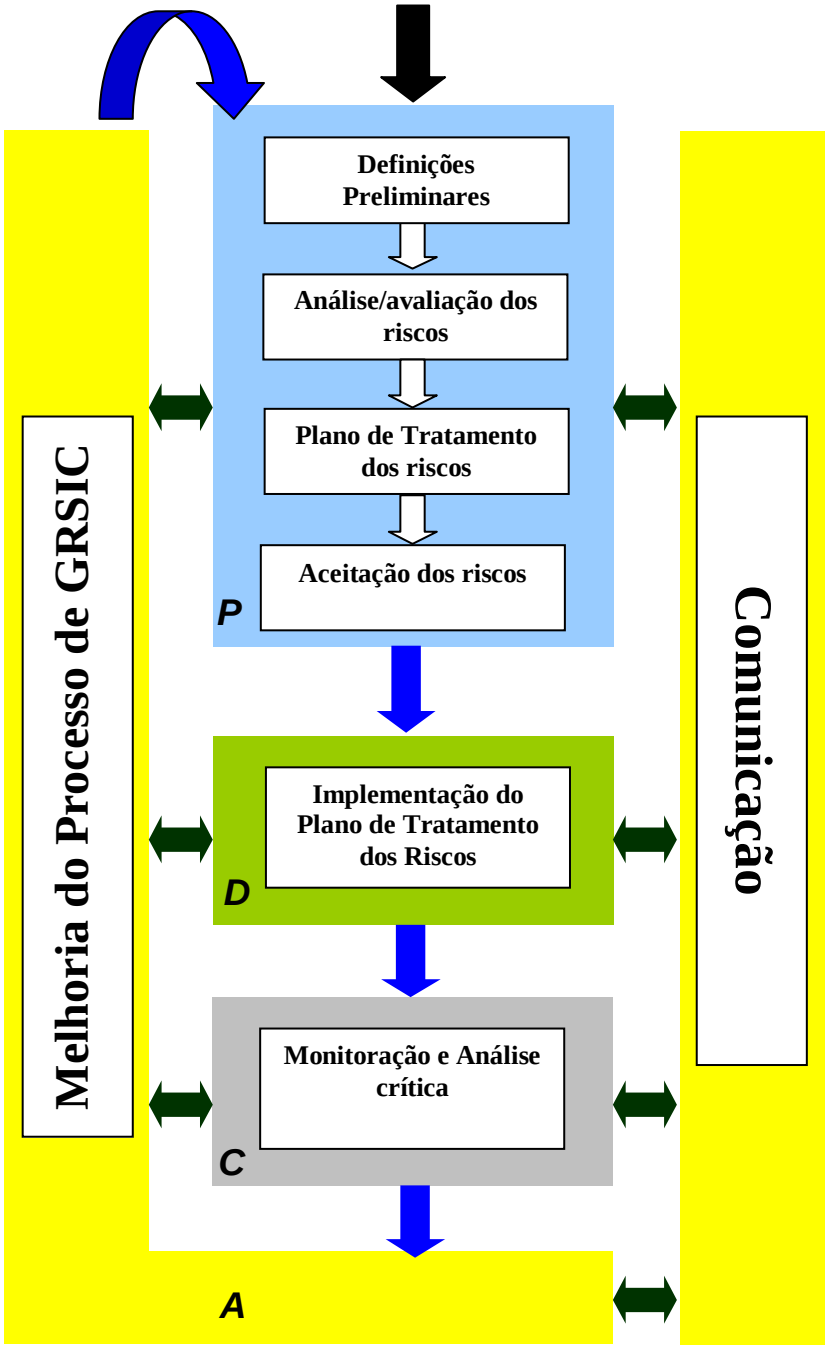
Esta Norma entra em vigor na data de sua publicação.

8 ANEXO

A - Processo de Gestão de Riscos de Segurança da Informação e Comunicações

ANEXO A

PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES



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

CRIAÇÃO DE EQUIPES DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS - ETIR

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 Anexo I do Decreto nº 5.772, de 8 de maio de 2006.
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.
Incisos II e IV do art. 37 da Portaria nº 13 do Gabinete de Segurança Institucional, de 4 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 a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

2 CONSIDERAÇÕES INICIAIS

2.1 Nos últimos anos os órgãos públicos vêm implementando e consolidando redes locais de computadores cada vez mais amplas, como exigência para suportar o fluxo crescente de informações, bem como permitir que seus funcionários acessem à rede mundial de computadores para melhor desempenharem suas funções. Manter a segurança da informação e comunicações de uma organização em um ambiente computacional interconectado nos dias atuais é um grande desafio, que se torna mais difícil à medida que são lançados novos produtos para a Internet e novas ferramentas de ataque são desenvolvidas.

2.2 Diante da premissa de garantir e incrementar a segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta, há a necessidade de orientar a condução de políticas de segurança já existentes ou a serem implementadas.

2.3 Considerando a estratégia de segurança da informação composta por várias camadas, uma delas, que vem sendo adotada por diversas instituições, é a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais, mundialmente conhecido como CSIRT® (do inglês "Computer Security Incident Response Team").

2.4 É competência da Coordenação-Geral de Tratamento de Incidentes de Redes do Departamento de Segurança da Informação e Comunicações – DSIC do Gabinete de Segurança Institucional – GSI apoiar os órgãos e entidades da Administração Pública Federal, direta e indireta, nas atividades de capacitação e tratamento de incidentes de segurança em redes de computadores, conforme disposto nos incisos III e VI do art. 39 do anexo da Portaria nº 13 do GSI, de 04 de agosto de 2006.

2.5 É condição necessária para a criação de uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, o órgão ou entidade possuir a competência formal e respectiva atribuição de administrar a infra-estrutura da rede de computadores de sua organização.

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 são estabelecidos os seguintes conceitos e definições:

4.1 **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 Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

4.2 **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;

4.3 **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;

4.4 **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;

4.5 **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;

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

4.7 **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;

4.8 **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;

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

5 RESPONSABILIDADE

Os Gestores de Segurança da Informação e Comunicações são os responsáveis por coordenar a instituição, implementação e manutenção da infraestrutura necessária às Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais, nos órgãos e entidades da Administração Pública Federal, direta e indireta, conforme descrito no inciso V do art 5º da Instrução Normativa nº 01, do Gabinete de Segurança Institucional, de 13 de junho de 2008.

6 DEFINIÇÃO DA MISSÃO

6.1 A missão deve fornecer uma breve e inequívoca descrição dos objetivos básicos e a função da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais. A definição da missão fornecerá a linha base para as atividades a serem desenvolvidas pela Equipe.

6.2 Recomenda-se como missão prioritária para a Equipe a facilitação e a coordenação das atividades de tratamento e resposta a incidentes em redes computacionais, além de alguma outra missão específica, em consonância com as atividades de resposta e tratamento a incidentes em redes, tais como: recuperação de sistemas, análise de ataques e intrusões, cooperação com outras equipes, participação em fóruns e redes nacionais e internacionais.

6.3 A definição da missão, juntamente com os serviços a serem prestados pela Equipe, influenciará o modelo de implementação mais adequado à necessidade da organização.

6.4 As missões da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais deverão ser descritas no respectivo documento de sua constituição, conforme o Anexo A desta Norma Complementar.

7 MODELO DE IMPLEMENTAÇÃO

Cada órgão ou entidade deverá estabelecer, dentre os modelos apresentados abaixo, aquele que melhor se adequar às suas necessidades e limitações, ressalvado que, independentemente do modelo escolhido, deverão ser observadas as diretrizes desta Norma Complementar. Nada obstante, em quaisquer dos modelos estabelecidos deverá ser designado formalmente o Agente Responsável, que terá, dentre outras atribuições, a de ser a interface com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV. Este Agente será o responsável por criar os procedimentos internos, gerenciar as atividades e distribuir tarefas para a Equipe ou Equipes que compõem a ETIR.

7.1 Modelo 1 – Utilizando a equipe de Tecnologia da Informação – TI

7.1.1 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.

7.1.2 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.

7.2 Modelo 2 – Centralizado

7.2.1 A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais será estabelecida de forma centralizada no âmbito da organização.

7.2.2 A Equipe será composta por pessoal com dedicação exclusiva às atividades de tratamento e

resposta aos incidentes em redes computacionais.

7.3 Modelo 3 – Descentralizado

7.3.1 No modelo descentralizado a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais será composta por colaboradores distribuídos por diversos locais dentro da organização, dispersos por uma região ou pelo país inteiro. Essas equipes devem possuir pessoal próprio dedicado às atividades de tratamento e resposta aos incidentes de rede computacionais, podendo atuar operacionalmente de forma independente, porém alinhadas com as diretrizes estabelecidas pela coordenação central.

7.3.2 A ETIR da organização será formada pelo conjunto dessas equipes distribuídas e chefiada pelo Agente Responsável designado.

7.4 Modelo 4 – Combinado ou Misto

7.4.1 Trata-se da junção dos modelos Descentralizado e Centralizado. Neste modelo existirá uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais central e Equipes distribuídas pela organização.

7.4.2 A Equipe central será a responsável por criar as estratégias, gerenciar as atividades e distribuir as tarefas entre as Equipes descentralizadas, além de ser a responsável, perante toda a organização, pela comunicação com o CTIR GOV.

7.4.3 As Equipes distribuídas serão responsáveis por implementar as estratégias e exercer suas atividades em suas respectivas áreas de responsabilidade.

8 ESTRUTURA ORGANIZACIONAL

8.1 Existem muitas maneiras diferentes de uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais ser estruturada. A estrutura dependerá do modelo de implementação a ser adotado, do tamanho da organização, do número de localizações geográficas distribuídas e onde as funções estão localizadas, do número de sistemas e plataformas suportadas, do número de serviços a serem oferecidos e do conhecimento técnico do pessoal existente.

8.2 Os membros da Equipe deverão ser selecionados, sempre que possível, dentre o pessoal existente, com perfil técnico adequado às funções de tratamento de incidentes de rede, os quais deverão dedicar o tempo integral, ou um percentual do seu tempo de trabalho, dependendo do modelo de implementação adotado, de forma reativa e pró-ativa.

8.3 O percentual do esforço dedicado será negociado entre a supervisão de cada um dos membros e o Agente Responsável pela Equipe e deverá estar descrito no documento de constituição da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

8.4 Recomenda-se que os membros da ETIR sejam: administradores de sistema ou de segurança, administradores de banco de dados, administradores de rede, analistas de suporte ou quaisquer outras pessoas da organização com conhecimento técnico comprovado. A Equipe poderá ser

estendida com a inclusão dos seguintes membros: representantes legais de áreas específicas da organização, advogados, estatísticos, recursos humanos, relações públicas, gestão de riscos, controle interno e grupo de investigação, ou outro que a organização entenda ser adequado.

8.5 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.

8.6 O Gestor de Segurança da Informação e Comunicações da organização será o responsável por prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da Equipe, bem como prover a infraestrutura necessária.

9 AUTONOMIA DA ETIR

A autonomia da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR descreve o escopo de atuação e o nível de responsabilidade que a Equipe tem sobre as suas próprias ações e sobre as atividades de resposta e tratamento dos incidentes na rede de computadores. A autonomia define o nível de controle da Equipe no relacionamento com os componentes da sua organização. A autonomia deverá ser definida, explicitamente, no documento de constituição da ETIR, conforme apresentado no Anexo A desta Norma.

9.1 Autonomia Completa

Se uma ETIR tem plena autonomia, ela poderá conduzir o seu público alvo para realizar ações ou as medidas necessárias para reforçar a resposta ou a postura da organização na recuperação de incidentes de segurança. Durante um incidente de segurança, se tal se justificar, a Equipe poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

9.2 Autonomia Compartilhada

9.2.1 Se a ETIR possui a autonomia compartilhada, ela trabalhará em acordo com os outros setores da organização a fim de participar do processo de tomada de decisão sobre quais medidas devam ser adotadas.

9.2.2 A ETIR participará no resultado da decisão, sendo, no entanto, apenas um membro no processo decisório. Neste caso, 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 os outros membros da organização.

9.2.3 A indicação dos membros do processo decisório deverá ser definida explicitamente no documento de constituição da ETIR.

9.3 Sem Autonomia

9.3.1 Se uma Equipe não tem autonomia, só poderá agir com a autorização de um membro da organização com a autoridade para tal, designado no documento de constituição da ETIR.

9.3.2 A ETIR não terá autonomia para a tomada de decisões ou adoção de ações, podendo, no entanto, recomendar os procedimentos a serem executados ou as medidas de recuperação durante um ataque, mas não terá um voto na decisão final.

9.3.3 A ETIR poderá ser capaz, devido à sua posição na organização e capacidade técnica, de conduzir os tomadores de decisão a agir durante um incidente de segurança, ressalvado o caráter sugestivo das recomendações.

10 DISPOSIÇÕES GERAIS

10.1 Os órgãos ou entidades que inicialmente optarem pela implantação do Modelo 1 (Utilizando a equipe de Tecnologia da Informação) deverão, assim que possível, migrar para um dos outros modelos.

10.2 Preferencialmente a Equipe deve ser composta por servidores públicos ocupantes de cargo efetivo ou militares de carreira, conforme o caso, com perfil técnico compatível, lotados nos seus respectivos órgãos.

10.3 Cada órgão poderá deliberar o nome de sua Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

10.4 A ETIR deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede orientados pelo Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV.

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

10.6 A ETIR deverá comunicar de imediato a ocorrência de todos os incidentes de segurança ocorridos na sua área de atuação ao CTIR GOV, conforme padrão definido por esse órgão, a fim de permitir a geração de estatísticas e soluções integradas para a Administração Pública Federal.

10.7 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.

11 VIGÊNCIA

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

12 ANEXO

A – DOCUMENTO DE CONSTITUIÇÃO DA ETIR.

ANEXO A

DOCUMENTO DE CONSTITUIÇÃO DA ETIR

A fim de regulamentar o funcionamento da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR, os órgãos e entidades da Administração Pública Federal, direta e indireta – APF deverão elaborar e publicar o Documento de Constituição da ETIR, alinhado com a Política de Segurança da Informação e Comunicações, devidamente aprovado pela Alta Administração do órgão ou entidade.
No documento de constituição da ETIR deverão constar, no mínimo, os seguintes pontos: definição da missão, comunidade ou público alvo, modelo de implementação escolhido, estrutura organizacional, autonomia e serviços que serão prestados.

1 MISSÃO

A missão deve fornecer uma breve e inequívoca descrição dos objetivos básicos e a função da ETIR. A organização deve observar o previsto no item 6 desta Norma Complementar e as seguintes premissas no que se refere à definição da missão:

1.1 Não deve conter termos ambíguos;

1.2 Não deve ser extensa, descrevendo de forma sucinta a missão da ETIR;

1.3 Deve ajudar a Equipe a entender os seus objetivos;

1.4 Deve complementar a missão do órgão ao qual pertence;

1.5 Deve estar alinhada à Política de Segurança da Informação e Comunicações do órgão ou entidade.

2 COMUNIDADE OU PÚBLICO ALVO

2.1 Deve ser formada pelos usuários da rede de computadores e sistemas do(s) órgão(ãos) ou entidade(s) atendidos pela ETIR.

2.2 Deve ser descrito o público com o qual a Equipe irá se relacionar, principalmente quando este não for composto por todos os integrantes do próprio órgão ou entidade, além da forma e as condições nas quais a comunicação será realizada.

2.3 Devem ser descritos ainda os relacionamentos com outros organismos de tratamento de incidente e as condições deste relacionamento.

3 MODELO DE IMPLEMENTAÇÃO

Cada órgão ou entidade deve estabelecer o modelo que melhor se adequar às suas necessidades e limitações, dentre os apresentados no item 7 desta Norma Complementar, descrevendo o modelo de forma detalhada e a maneira de atuação da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais dentro da organização.

4 ESTRUTURA ORGANIZACIONAL

Observadas as diretrizes constantes no item 8 desta Norma Complementar, deve ser definida a estrutura organizacional da ETIR, nos seguintes termos:

4.1 Posição na estrutura organizacional do órgão a que pertence;

4.2 Definição do Agente Responsável pela ETIR, suas competências, atribuições e responsabilidades perante o Gestor de Segurança da Informação e Comunicações, as demais esferas decisórias da organização e o CTIR GOV;

4.3 Definição da Equipe e/ou Equipes descentralizadas, seus membros componentes e membros agregados, suas funções, responsabilidades, maneira de atuação e tempo destinado às tarefas da ETIR;

4.4 Definição dos membros substitutos, suas atribuições e responsabilidades.

5 AUTONOMIA DA ETIR

5.1 Na definição da autonomia da ETIR o órgão ou entidade deve observar as diretrizes constantes no item 9 desta Norma Complementar.

5.2 Devem ser definidos explicitamente o modelo adotado, o escopo de atuação, o nível de responsabilidade e a independência da Equipe sobre as ações necessárias à resposta e tratamento dos incidentes de segurança na rede de computadores, divulgando para toda a organização.

5.3 Dependendo do nível de autonomia da ETIR, devem ser indicados os membros da organização com autoridade para decidir sobre as ações a serem adotadas.

6 SERVIÇOS

6.1 Para a definição dos serviços que serão prestados cada órgão deve observar as suas necessidades e limitações, a missão, o modelo de implementação adotado e a autonomia da ETIR, tudo em consonância com o que prescreve esta Norma Complementar.

6.2 Os serviços prestados por uma ETIR definem quais os procedimentos a Equipe desempenhará. Para cada serviço este documento deve descrever, no mínimo, os seguintes atributos:

6.2.1 Objetivo;

6.2.2 Definição;

6.2.3 Descrição das funções e procedimentos que compõem o serviço;

6.2.4 Disponibilidade do serviço: quando, como e onde o serviço será oferecido;

6.2.5 Metodologia para execução do serviço.

6.3 A ETIR deve implementar, no mínimo, o serviço de Tratamento de Incidentes de Segurança em Redes Computacionais. Este serviço, conforme sua definição, 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.

6.4 A Equipe poderá oferecer à sua comunidade ou público alvo, além do tratamento de incidentes, outros serviços correlacionados à resposta e tratamento de incidentes de segurança em redes computacionais, de acordo com normas nacionais e internacionais.

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

ORIENTAÇÕES ESPECÍFICAS PARA O USO DE RECURSOS CRIPTOGRÁFICOS EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

Decreto nº 3.505, de 13 de junho de 2000
Decreto nº 4.553, de 27 de dezembro de 2002
Instrução Normativa GSI 01 de 13 de junho de 2008
Norma Complementar 01/DSIC/GSIPR de 13 de outubro de 2008
Norma Complementar 02/DSIC/GSIPR de 13 de outubro de 2008
Norma Complementar 07/DSIC/GSIPR de 14 de abril de 2010

CAMPO DE APLICAÇÃO

Esta Norma 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 orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta (APF).

2 RESPONSABILIDADES

2.1 Caberá aos órgãos ou entidades da APF, no âmbito de suas competências, a utilização dos recursos criptográficos em conformidade com as orientações contidas nesta norma, sob pena de responsabilidade;

2.1.1 No âmbito de suas competências, os Gestores de Segurança da Informação e Comunicações são responsáveis pela implementação dos procedimentos relativos ao uso dos recursos criptográficos, em conformidade com as orientações contidas nesta norma, nos órgãos e entidades da Administração Pública Federal, direta e indireta;

2.1.2 O agente público ao receber um recurso criptográfico torna-se responsável pelo mesmo, devendo assinar o respectivo Termo de Uso de Recurso Criptográfico, conforme modelo constante no Anexo A.

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 TERMOS E DEFINIÇÕES

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

4.1- **Algoritmo de Estado**: função matemática utilizada na cifração e/ou decifração, de propriedade inequívoca do Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades da Administração Pública Federal, direta e indireta;

4.2 - **Chave criptográfica**: valor que trabalha com um algoritmo criptográfico para cifração e/ou decifração.

4.3 - **Cifração:** ato de cifrar mediante o uso de algoritmo simétrico ou assimétrico, utilizando recurso criptográfico, a fim de substituir sinais de uma linguagem clara por outros ininteligíveis para aqueles que não estejam autorizados a conhecê-la;

4.4 - **Decifração:** ato de decifrar mediante o uso de algoritmo simétrico ou assimétrico, utilizando recurso criptográfico, a fim de reverter o processo de cifração original;

4.5 - **Recurso Criptográfico:** sistemas, programas, processos e equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar a cifração ou decifração.

5 ORIENTAÇÕES ESPECÍFICAS

Para fins de utilização de recursos criptográficos pelos órgãos e entidades da Administração Pública Federal, direta e indireta, além da legislação aplicável, deverão ser observados os seguintes procedimentos:

5.1 Recomenda-se o uso de recursos criptográficos baseados em algoritmo de Estado para cifração e decifração nos órgãos e entidades da Administração Pública Federal, direta e indireta;

5.1.1 O agente público, quando da cifração ou decifração no exercício de cargo, função, emprego ou atividade nos órgão ou entidades da Administração Pública Federal, direta e indireta, deve utilizar recurso criptográfico baseado em algoritmo de Estado adotado pelo órgão ao qual está vinculado;

5.2 Os recursos criptográficos baseados em algoritmo de Estado utilizam parâmetros e/ou padrões estabelecidos pelo Gabinete de Segurança Institucional da Presidência da República, por intermédio do Departamento de Segurança da Informação e Comunicações – DSIC, em conjunto com o Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações – CEPESC da Agência Brasileira de Inteligência – ABIN;

5.3 O uso de recurso criptográfico baseado em algoritmo de Estado é restrito ao agente público e requer treinamento e credenciamento, sob responsabilidade dos órgãos e entidades da Administração Pública Federal, direta e indireta;

5.4 O credenciamento de estrangeiros para uso de recurso criptográfico baseado em algoritmo de Estado deve ser submetido ao Gabinete de Segurança Institucional da Presidência da República por intermédio do Departamento de Segurança da Informação e Comunicações – DSIC;

5.5 A cifração e decifração de informações classificadas e sigilosas devem utilizar recurso criptográfico baseado em algoritmo de Estado em conformidade com os parâmetros mínimos estabelecidos no Anexo B.

5.6 Todo recurso criptográfico constitui uma informação classificada sigilosa e requer procedimentos especiais de controle para o seu acesso, manutenção, armazenamento, transferência, trânsito e descarte, em conformidade com a legislação pertinente;

5.7 É vedado ao usuário de recurso criptográfico nos órgãos e entidades da Administração Pública Federal, direta e indireta:

5.7.1 utilizar recursos criptográficos em desacordo com esta norma, bem como com a legislação em vigor;

5.7.2 utilizar recursos criptográficos diferentes dos padrões definidos pelo órgão ou entidade da Administração Pública Federal, direta e indireta, a que pertence;

5.7.3 impedir ou dificultar, de qualquer forma, a realização das atividades de monitoramento e auditoria dos recursos criptográficos pertencentes ao órgão ou entidade da Administração Pública Federal, direta e indireta.

5.8 Além do disposto nesta norma, os recursos criptográficos que utilizam algoritmos no interesse da segurança e da defesa nacionais podem ser objeto de regulamentação específica.

6 VIGÊNCIA

Esta norma entra em vigor na data de sua publicação

ANEXO A

Modelo de Termo de Uso de Recurso Criptográfico

SERVIÇO PÚBLICO FEDERAL

(Nome do órgão ou entidade da APF)

TERMO DE USO DE RECURSO CRIPTOGRÁFICO

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em _____, e lotado no(a)_____deste (Nome do órgão ou entidade), DECLARO , sob pena das sanções cabíveis e nos termos da _____ (legislação vigente) que TENHO conhecimento sobre o uso do recurso criptográfico sob minha responsabilidade, sendo vedado seu uso:

I) para fins diversos dos funcionais ou institucionais;

II) para interceptar ou tentar interceptar transmissão de dados ou informações não destinados ao seu próprio acesso por quaisquer meios;

III) para tentar ou efetuar a interferência em serviços de outros usuários ou o seu bloqueio por quaisquer meios;

IV) para violar ou tentar violar os recursos de segurança dos equipamentos que utilizem recursos criptográficos;

V) para cifração ou decifração de informações ilícitas, entre os quais, materiais obscenos, ofensivos, ilegais, não éticos, ameaças, difamação, injúria, racismo ou quaisquer que venham a causar molestamento, tormento ou danos a terceiros;

VI) de forma inadequada, expondo-o a choques elétricos ou magnéticos, líquidos ou outros fatores que possam vir a causar-lhes danos, incluindo testes de invasão/intrusão/penetração, teste de quebra de senhas, teste de quebra de cifração, e teste de técnicas de invasão e defesa entre outros;

Local, UF, _____de _____de _____ .

_____

Assinatura

Nome do usuário e seu setor organizacional

ANEXO B

Parâmetros mínimos para algoritmo de Estado

TABELA I - Tamanho da chave:

Nível de segurança da Informação	RSA/LD	Curvas Elípticas
Reservado	2048	224
Confidencial	2048	224
Secreto	3248	256
Ultra Secreto	Não recomendado	Não recomendado

TABELA II - Algoritmos de bloco:

Classificação	Algoritmo de Estado	
	Chave	Bloco
Reservado	128	128
Confidencial	192	128
Secreto	256	128
Ultra-Secreto	Não recomendado	

TABELA III - Algoritmos seqüenciais:

Classificação	Algoritmo de Estado
Reservado	128
Confidencial	192
Secreto	256
Ultra Secreto	Não recomendado

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

GESTÃO DE CONTINUIDADE DE NEGÓCIOS EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

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 Anexo I do Decreto nº 6.931, de 11 de agosto de 2009.
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.
NBR 15999-1: 2007 – Gestão de Continuidade de Negócios.
NBR ISO/IEC 27002 (17799:2005)
Cobit 4.1 DS4 *Ensure Continuous Service*

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 Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

2 CONSIDERAÇÕES INICIAIS

A implantação do processo de Gestão de Continuidade de Negócios busca minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão ou entidade, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

A Gestão de Continuidade de Negócios pode envolver ações mais abrangentes do que as definidas no âmbito da Gestão de Segurança da Informação e Comunicações, especialmente devido aos requisitos estratégicos de continuidade relativos às pessoas, à infraestrutura, aos processos e às atividades operacionais.

A Gestão de Continuidade de Negócios, objeto desta norma complementar, está limitada ao escopo das ações de Segurança da Informação e Comunicações implementadas nos órgãos ou entidades da APF.

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, aplicam-se os seguintes conceitos e definições:

4.1 **Atividade:** processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

4.2 **Atividades Críticas**: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo.

4.3 **Análise de Impacto nos Negócios (AIN):** visa estimar os impactos resultantes da interrupção de serviços e de cenários de desastres que possam afetar o desempenho dos órgãos

ou entidades da APF, bem como as técnicas para quantificar e qualificar esses impactos. Define também a criticidade dos processos de negócio, suas prioridades de recuperação, interdependências e os requisitos de segurança da informação e comunicações para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos

4.4 **Ativos de informação:** os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

4.5 **Continuidade de Negócios**: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

4.6 **Desastre**: Evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;

4.7 **Estratégia de Continuidade de Negócios:** abordagem de um órgão ou entidade que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou outro incidente maior;

4.8 **Gestão de Continuidade**: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado;

4.9 **Incidente:** evento que tenha causado algum dano, colocado em risco, algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

4.10 **Plano de Continuidade de Negócios:** documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da APF mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes;

4.11 **Plano de Gerenciamento de Incidentes**: plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;

4.12 **Plano de Recuperação de Negócios:** documentação dos procedimentos e informações necessárias para que o órgão ou entidade da APF operacionalize o retorno das atividades críticas a normalidade;

4.13 **Programa de Gestão da Continuidade de Negócios:** processo contínuo de gestão e governança suportado pela alta direção e que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por intermédio análises críticas, testes, treinamentos e manutenção;

4.14 **Tempo Objetivo de Recuperação:** é o tempo pré-definido no qual uma atividade deverá estar disponível após uma interrupção ou incidente;

4.15 **Resiliência:** poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre.

5 PROCEDIMENTOS

5.1 A elaboração do Programa de Gestão da Continuidade de Negócios envolve os seguintes procedimentos:

5.1.1 desenvolver documento com as diretrizes do Programa de Continuidade;

5.1.2 definir as atividades críticas do órgão ou entidade;

5.1.3 avaliar os riscos a que estas atividades críticas estão expostas;

5.1.4 definir as estratégias de continuidade para as atividades críticas;

5.1.5 desenvolver e implementar os Planos previstos no Programa de Gestão da Continuidade de Negócios para respostas tempestivas a interrupções;

5.1.6 realizar exercícios, testes e manutenção periódica dos Planos, promovendo as revisões necessárias;

5.1.7 desenvolver a cultura de continuidade de negócios no órgão ou entidade;

5.2 Os procedimentos previstos no Programa de Gestão da Continuidade de Negócios são executados em conformidade com os requisitos de segurança da informação e comunicações necessários à proteção dos ativos de informação críticos, tratando as atividades de forma abrangente, o que inclui as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação e comunicações;

5.3 Recomenda-se que o Programa de Gestão de Continuidade de Negócios de um órgão ou entidade da APF seja composto, no mínimo, pelos seguintes Planos, de acordo com as suas necessidades específicas, de forma a assegurar a disponibilidade dos ativos de informação e a recuperação das atividades críticas:

5.3.1 Plano de Gerenciamento de Incidentes - PGI;

5.3.2 Plano de Continuidade de Negócios - PCN;
5.3.3 Plano de Recuperação de Negócios - PRN.

5.4 Cada um dos Planos contém, no mínimo:

5.4.1 Plano de Gerenciamento de Incidentes:
a) Objetivo e escopo;
b) Papéis e responsabilidades;
c) Condições para a ativação de Planos;
d) Autoridade responsável;
e) Detalhes de contato;
f) Lista de tarefas e ações;
g) Atividades das pessoas;
h) Comunicação à mídia;
i) Localização para o gerenciamento de incidentes.

5.4.2 Plano de Continuidade de Negócios:
a) Objetivo e escopo;
b) Papéis e responsabilidades;
c) Autoridade responsável;
d) Detalhes de contato;
e) Lista de tarefas;
f) Recursos necessários.

5.4.3 Plano de Recuperação de Negócios:
a) Objetivo e escopo;
b) Papéis e responsabilidades;
c) Autoridade responsável;
d) Detalhes de contato;
e) Lista de tarefas;
f) Recursos necessários.

5.5 Os Planos são exercitados e testados periodicamente, bem assim os resultados documentados de forma a garantir a sua efetividade.

5.6 A revisão dos Planos é realizada nas seguintes situações:

5.6.1 No mínimo, uma vez por ano;

5.6.2 Em função dos resultados dos testes realizados; ou

5.6.3 Após alguma mudança significativa nos ativos de informação, nas atividades ou em algum de seus componentes.

5.7 Sugere-se que os contratos firmados com empresas terceirizadas que suportem atividades críticas contenham cláusula segundo a qual as referidas empresas possuam Planos de Continuidade dos seus Negócios, bem como as evidências dos testes realizados.

6 RESPONSABILIDADES

6.1 Para a Alta Administração do órgão ou entidade da APF, no âmbito de suas atribuições, recomenda-se que sejam adotadas as seguintes responsabilidades:

6.1.1 aprovar as diretrizes estratégicas que norteiam a elaboração do Programa de Gestão de Continuidade de Negócios;

6.1.2 avaliar a relação custo / benefício das estratégias de continuidade propostas e dos Planos que compõem o Programa de Gestão da Continuidade de Negócios e decida sobre sua implementação;

6.1.3 garantir os recursos necessários para estabelecer, implementar, operar e manter o Programa de Gestão da Continuidade de Negócios.

6.2 As seguintes atribuições devem ser conferidas ao responsável pela Gestão da Continuidade de Negócios, ou ao Gestor de Segurança da Informação e Comunicações, no caso do órgão ou entidade não possuir o Gestor de Continuidade de Negócios;

6.2.1 Propor as diretrizes estratégicas do Programa de Gestão da Continuidade de Negócios;

6.2.2 Avaliar o plano de tratamento de riscos;

6.2.3 Realizar, periodicamente, a Análise de Impacto nos Negócios (AIN);

6.2.4 Propor melhorias na implantação de novos controles relativos ao Programa de Gestão de Continuidade de Negócios;

6.2.5 Supervisionar a elaboração, implementação, testes e atualização dos Planos;

6.2.6 Desenvolver a cultura de Gestão de Continuidade de Negócios.

6.3 As seguintes atribuições devem ser conferidas aos responsáveis pelos setores ou processos onde foram identificadas atividades críticas para o órgão ou entidade da APF:

6.3.1 Elaborar os Planos previstos no Programa de Gestão da Continuidade de Negócios relacionados às atividades críticas;

6.3.2 Realizar os testes e exercícios dos Planos;

6.3.3 Avaliar e aprimorar os Planos a partir dos resultados dos testes e exercícios;

6.3.4 Administrar a contingência quando da interrupção de atividades, com base nos Planos desenvolvidos;

6.3.5 Propor os recursos necessários para a implantação e o desenvolvimento das ações relacionadas à continuidade das atividades, bem como para a realização dos testes e dos exercícios dos Planos.

7 **VIGÊNCIA**

Esta Norma entra em vigor na data de sua publicação, gerando seus efeitos a partir de 17 de maio de 2010.

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

DIRETRIZES PARA IMPLEMENTAÇÃO DE CONTROLES DE ACESSO RELATIVOS À SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES.

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA LEGAL E NORMATIVA

Art. 6º da Lei nº 10.683, de 28 de maio de 2003;
Art. 8º do Anexo I do Decreto nº 6.931, de 11 de agosto de 2009;
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 e suas Normas Complementares;
NBR ISO/IEC 27001:2006 – Sistema de Gestão de segurança da informação;
NBR ISO/IEC 27002:2005 – Código de Práticas para a Gestão da Segurança da Informação;

CAMPO DE APLICAÇÃO

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

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Anexo: Não há

APROVAÇÃO

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

1. OBJETIVO

Estabelecer 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.

2. CONSIDERAÇÕES INICIAIS

2.1.O objetivo do controle é sistematizar a concessão de acesso, a fim de evitar a quebra de segurança da informação e comunicações.

2.2.A identificação, a autorização, a autenticação, o interesse do serviço e a necessidade de conhecer são condicionantes prévias para concessão de acesso nos órgãos ou entidades da APF.

2.3.A identificação dos controles de acesso lógico e físico, nos órgão ou entidade da APF, é consequência do processo de Gestão de Riscos de Segurança da Informação e Comunicações.

2.4.A implementação dos controles de acesso está condicionada à prévia aprovação pela autoridade responsável pelo órgão ou entidade da APF.

2.5.Para implementar os controles de acesso aprovados é fundamental a elaboração e divulgação de normas, bem como programas periódicos de sensibilização e conscientização em conformidade com a Política de Segurança da Informação e Comunicações dos órgãos ou entidades da APF.

2.6.Os órgãos ou entidades da APF, em suas áreas de competência, estabelecem regras específicas para credenciamento de acesso de usuários aos ativos de informação em conformidade com a legislação vigente, e em especial quanto ao acesso às informações em áreas e instalações consideradas críticas.

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 são estabelecidos 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.**Ativos de informação** - os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

4.3.**Bloqueio de acesso**: processo que tem por finalidade suspender temporariamente o acesso.

4.4.**Contas de Serviço**: contas de acesso à rede corporativa de computadores necessárias a um procedimento automático (aplicação, script, etc.) sem qualquer intervenção humana no seu uso.

4.5.**Controle de acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.

4.6.**Credenciamento**: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer.

4.7.**Credenciais ou contas de acesso**: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha.

4.8.**Exclusão de acesso**: processo que tem por finalidade suspender definitivamente o acesso, incluindo o cancelamento do código de identificação e do perfil de acesso.

4.9.**Gestão de Riscos de Segurança da Informação e Comunicações** – conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

4.10. **Necessidade de conhecer** - condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação.

4.11. **Perfil de acesso**: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso.

4.12. **Prestador de serviço**: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso.

4.13. **Quebra de segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações;

4.14. **Termo de Responsabilidade**: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso (Modelo - Anexo A).

4.15. **Tratamento da informação**: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

4.16. **Usuário**: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade.

5. DIRETRIZES PARA CONTROLE DE ACESSO LÓGICO

5.1 Quanto à criação e administração de contas de acesso:

5.1.1 A criação de contas de acesso aos ativos de informação requer procedimentos prévios de credenciamento para qualquer usuário.

5.1.2 Disponibilizar ao usuário, que não exerce funções de administração da rede local, somente uma única conta institucional de acesso, pessoal e intransferível.

5.1.3 Utilizar conta de acesso no perfil de administrador somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

5.1.4 Responsabilizar o usuário pela quebra de segurança ocorrida com a utilização de sua respectiva conta de acesso, mediante assinatura de Termo de Responsabilidade (Modelo - Anexo A).

5.1.5 A criação de contas de serviço exige regras específicas vinculadas a um processo automatizado.

5.1.6 Os órgãos ou entidades da APF, em suas áreas de competência, estabelecem regras para credenciamento, bloqueio e exclusão de contas de acesso de seus usuários, bem como para o ambiente de desenvolvimento.

5.2 Quanto à rede corporativa de computadores:

5.2.1 Conceder credenciais de acesso à rede corporativa de computadores após a data de contratação ou de entrada em exercício do usuário.

5.2.2 Excluir credenciais de acesso à rede corporativa de computadores quando do desligamento do usuário.

5.2.3 Registrar os acessos à rede corporativa de computadores de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido em cada órgão ou entidade da APF.

5.2.4 Implementar, sempre que possível, pelo menos um dos mecanismos que contemplam biometria, tokens, smart cards, a fim de autenticar a identidade do usuário da rede.

5.2.5 Utilizar mecanismos automáticos para inibir que equipamentos externos se conectem na rede corporativa de computadores.

5.2.6 Manter, na rede corporativa, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados.

5.2.7 Utilizar a legislação específica para a concessão de acesso às informações sigilosas e para o acesso remoto, no âmbito da rede corporativa, por meio de canal seguro.

5.2.8 Gravar o acesso remoto à rede corporativa em logs para posterior auditoria, contendo informações específicas que facilitem o rastreamento da ação tomada;

5.2.9 Os órgãos ou entidades da APF, em suas áreas de competência, estabelecem regras para o uso de redes sem fio.

5.3 Quanto aos ativos de informação:

5.3.1 Conter ferramentas de proteção contra acesso não autorizado aos ativos de informação, que favoreça, preferencialmente, a administração de forma centralizada.

5.3.2 Respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação;

5.3.3 Utilizar ativo de informação homologado nas aplicações de controle de acesso, de tratamento das informações sigilosas e de criptografia;

5.3.4 Registrar eventos relevantes, previamente definidos, para a segurança e rastreamento de acesso às informações sigilosas.

5.3.5 Criar mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

5.3.6 O uso dos ativos de informação que não guarde relação com o exercício do cargo, função, emprego ou atividade públicas será considerado indevido e passível de imediato bloqueio de acesso, sem prejuízo da apuração das responsabilidades administrativa, penal e civil.

5.3.7 Os órgãos ou entidades da APF, em suas áreas de competência, estabelecem regras para o uso da Internet, do Correio Eletrônico e de Mensagens Instantâneas.

6. DIRETRIZES PARA CONTROLE DE ACESSO FÍSICO

6.1 Quanto às áreas e instalações físicas:

6.1.1 Os Órgãos ou entidades da APF estabelecem regras para o uso de credenciais físicas (crachá, botom, cartões, selos, etc,), que se destinam ao controle de acesso dos usuários às áreas e instalações sob suas responsabilidades;

6.1.2 Os Órgãos ou entidades da APF definem a necessidade e orientam a instalação de sistemas de detecção de intrusos nas áreas e instalações sob suas responsabilidades;

6.1.3 Classificar as áreas e instalações como ativos de informação de acordo com o valor, a criticidade, o tipo de ativo de informação e o grau de sigilo das informações que podem ser tratadas em tais áreas e instalações, mapeando aquelas áreas e instalações consideradas críticas;

6.1.4 Os Órgãos ou entidades da APF orientam o uso de barreiras físicas de segurança, bem como equipamentos ou mecanismos de controle de entrada e saída;

6.1.5 Proteger os ativos de informação contra ações de vandalismo, sabotagem, ataques, etc, especialmente em relação àqueles considerados críticos.

6.1.6 Implementar área de recepção com regras claras para a entrada e saída de pessoas, equipamentos e materiais;

6.1.7 Definir pontos de entrega e carregamento de material com acesso exclusivo ao pessoal credenciado;

6.1.8 Intensificar os controles para as áreas e instalações consideradas críticas em conformidade com a legislação vigente.

6.2 Quanto aos usuários:

6.2.1 Difundir e exigir o cumprimento da Política de Segurança da Informação e Comunicações, das normas de segurança e da legislação vigente acerca do tema;

6.2.2 Conscientizar o usuário para adotar comportamento favorável à disponibilidade, à integridade, à confidencialidade e à autenticidade das informações.

6.2.3 Identificar e avaliar sistematicamente os riscos à segurança da informação e comunicações dos ativos de informação e quais controles devem ser aplicados quanto aos acessos dos usuários;

6.2.4 Estabelecer formulário específico de Termo de Responsabilidade (Modelo - Anexo A) a ser difundido e assinado individualmente pelos usuários;

6.2.5 Definir regras específicas para autorização de acesso e credenciamento dos usuários em conformidade com a classificação dos ativos de informação.

6.3 Quanto aos ativos de informação:

6.3.1 Estabelecer distância mínima de segurança para manutenção das mídias contendo as cópias de segurança (backups);

6.3.2 Classificar os ativos de informação em níveis de criticidade, considerando o tipo de ativo de informação, o provável impacto no caso de quebra de segurança, tomando como base a gestão de risco e a gestão de continuidade de negócios relativas aos aspectos da segurança da informação e comunicações da APF,

6.3.3 Um exemplo para classificação dos ativos de informação está disposto no Anexo B.

6.3.4 Os ativos de informação classificados como sigilosos requerem procedimentos especiais de controles de acesso físico em conformidade com a legislação vigente.

6.4 Quanto ao perímetro de segurança:

6.4.1 Definir perímetros de segurança, suas dimensões, equipamentos e tipos especiais de controles de acesso aos ativos de informação;

6.4.2 Ilustrar em documentação própria e permitir que sejam identificados os perímetros de segurança de cada ativo de informação por todos que transitarem ou tiverem acesso em tais espaços, em especial às áreas e instalações consideradas críticas;

6.4.3 Regulamentar, por intermédio de normas específicas de cada órgão ou entidade da APF, o armazenamento, a veiculação de imagem, vídeo ou áudio, registrados em perímetros de segurança.

7 VIGÊNCIA

Esta norma entra em vigor na data de sua publicação.

ANEXO A – Modelo de Termo de Responsabilidade

SERVIÇO PÚBLICO FEDERAL

(Nome do órgão ou entidade da APF)

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em _____, e lotado no(a)_____deste (Nome do órgão ou entidade), DECLARO , sob pena das sanções cabíveis nos termos da _____ (legislação vigente) que assumo a responsabilidade por:

I) tratar o(s) ativo(s) de informação como patrimônio do (Nome do órgão ou entidade);

II) utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do (Nome do órgão ou entidade);

III) contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;

IV) utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do (Nome do órgão ou entidade);

V) responder, perante o (Nome do órgão ou entidade), pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

Local, UF, _____de _____de _____ .

_____

Assinatura

Nome do usuário e seu setor organizacional

_____

Assinatura

Nome da autoridade responsável pela autorização do acesso

ANEXO B - Modelo de Classificação de Ativos de Informação

Grau de criticidade	Ativos de informação	Impacto	Cor
Nível 1 – Alto	Data-center, servidores, central telefônica, recursos criptológicos, cópias de segurança, equipamentos de conectividade ou de armazenamento de informações ou de computação móvel das autoridades de primeiro escalão.	Interrompe a missão do órgão ou provoca grave dano à imagem institucional, à segurança do estado ou sociedade.	Vermelha
Nível 2 – Médio	Computadores com dados e informações únicas, de grande relevância, equipamentos de conectividade ou de armazenamento de informações ou de computação móvel das autoridades de segundo escalão.	Degrada o serviço do órgão ou provoca dano à imagem institucional, à segurança do estado ou sociedade.	Amarela
Nível 3 – Baixo	Os demais ativos de informação	Compromete planos ou provoca danos aos ativos de informação.	Sem cor

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.