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.