GABINETE DE SEGURANÇA INSTITUCIONAL

PORTARIA No- 34, DE 13 DE OUTUBRO DE 2008
Homologa a Norma Complementar nº 02/DSIC/GSIPR

O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, na condição de **SECRETÁRIO-EXECUTIVO DO CONSELHO DE DEFESA NACIONAL**, no uso da atribuição que lhe confere o Decreto nº 3.505, de 13 de junho de 2000, e o Decreto nº 5.772, de 8 de maio de 2006;

RESOLVE:

Art. 1º Fica homologada a Norma Complementar nº 02/DSIC/GSIPR aprovada pelo Departamento de Segurança da Informação e Comunicações, em anexo.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

JORGE ARMANDO FELIX

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.