**MINISTÉRIO DA INTEGRAÇÃO NACIONAL**

# POLÍTICA DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E DAS COMUNICAÇÕES

PRINCÍPIOS E DIRETRIZES

JUNHO, 2013.

# Sumário

# 1. POLÍTICA DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E DAS COMUNICAÇÕES DO MINISTÉRIO DA INTEGRAÇÃO NACIONAL

## 1.1. ESCOPO

A Política de Gestão de Riscos de Segurança da Informação e das Comunicações (PGRSIC) tem por finalidade apresentar e estabelecer princípios, diretrizes e responsabilidades relacionados à Gestão de Riscos de Segurança da Informação e das Comunicações para o Ministério da Integração Nacional (MI).

A Política de Gestão de Riscos de Segurança da Informação e das Comunicações obedecerá aos princípios constitucionais, administrativos e ao arcabouço legislativo vigente que rege a Administração Pública Federal.

O objetivo da PGRSIC é orientar o planejamento, a implementação e a manutenção do processo de Gestão de Riscos da Segurança da Informação e das Comunicações segundo a metodologia preconizada pela Norma ABNT NBR ISO/IEC 27005 – Gestão de Riscos de Segurança e Tecnologia da Informação, de 2011, e dispositivos da Norma Complementar 04/IN01/DSIC/GSI/PR, de 15 de fevereiro de 2013, associando, dessa forma, o processo de Gestão de Riscos à tomada de decisões estratégicas da Organização, em conformidade com as boas práticas recomendadas pelos órgãos de controle da Administração Pública Federal.

## 1.2. ABRANGÊNCIA

Esta Política aplica-se a todos os membros, servidores e estagiários do MI e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional do Ministério da Integração Nacional.

Esta Política define responsabilidades para a Gestão de Riscos de Segurança da Informação e das Comunicações (GRSIC), bem como para a atualização da documentação pertinente.

Esta Política fomenta, ao longo de toda a estrutura organizacional do MI, a obtenção de atitude favorável no tocante à GRSIC, bem como incrementar a conscientização a respeito da importância do assunto.

## 1.3. CONCEITOS E DEFINIÇÕES

Para os fins desta Política, consideram-se os conceitos dos termos e expressões que constam do glossário de Segurança da Informação e das Comunicações e GRSIC.

Ameaça – conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
Análise/avaliação de riscos – processo completo de análise e avaliação de riscos;
Ativo – qualquer bem, tangível ou intangível, que tenha valor para a organização;
Ativo da 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;
Ativo Sigiloso – qualquer bem tangível ou intangível que possa conter informações sigilosas que, se acessadas por pessoas não autorizadas, podem causar danos significativos à organização;
Contingência – descrição de medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos à corporação;
DGE – Departamento de Gestão Estratégica;
Gestão de Risco – 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;
Gestor de Segurança da Informação e das Comunicações – é responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF;

Plano de Contingência – Descrever as medidas a serem tomadas por uma organização, incluindo a ativação de processos manuais, para fazer com que seus processos críticos voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada;
Plano de Continuidade de Negócios – Processo de gestão global que identifica as potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, se concretizando, poderiam causar, e fornecendo e mantendo um nível aceitável de serviço em face das rupturas e desafios à operação normal do dia-a-dia;

Política de Segurança da Informação e das Comunicações (POSIC) – 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;

Sistema de Segurança da Informação – proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento.

## 1.4. REFERÊNCIAS LEGAIS E NORMATIVAS

POSIC – Política de Segurança da Informação e das Comunicações do MI;

Decreto nº 7.724 de 16/05/2012, que regulamenta a Lei 12.527, de 18/11/2011 – Dispõe sobre o acesso a informações;

Instrução Normativa GSI nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal;

Norma Complementar nº 01/IN01/DSIC/GSIPR, Atividade de Normatização;

Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal;

Norma Complementar 04/IN01/DSIC/GSI/PR, de 15 de fevereiro de 2013, Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC;

Norma Complementar nº 06/IN01/DSIC/GSIPR, Estabelece 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;

Norma Complementar nº 10/IN01/DSIC/GSIPR, Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e das Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

ISO/IEC *Guide* 73:2002 – Gestão de Riscos / Vocabulário – Recomendações para uso em normas;

NBR/ISO/IEC 27002/2005, que institui o código de melhores práticas para gestão de segurança da informação;

NBR/ISO/IEC 27001/2006, que estabelece os elementos de um Sistema de Gestão de Segurança da Informação;

ABNT NBR ISO/IEC 27005 Gestão de Riscos de Segurança e Tecnologia da Informação, de 2011;
ABNT ISO/IEC GUIA 73: Gestão de Riscos – Vocabulário, de 2009.

## 1.5. PRINCÍPIOS

São princípios da PGRSIC:
1.5.1. Esta Política de Gestão de Riscos de Segurança da Informação e das Comunicações (PGRSIC) se aplica às atividades de todos os servidores, prestadores de serviços e fornecedores que venham a desempenhar atividades no âmbito do MI.

1.5.2. Responsabilidade: os agentes públicos devem conhecer e respeitar a PGRSIC do MI e devem ser responsabilizados pelos atos que coloquem em risco a segurança da informação;

1.5.3. Ética: os direitos dos agentes públicos devem ser preservados, sem expor o MI a ameaças de riscos de segurança da informação e das comunicações;

1.5.4. Celeridade: as ações de tratamento de riscos de segurança da informação e das comunicações devem oferecer respostas rápidas a incidentes e falhas de segurança;

1.5.5. Economicidade da proteção dos ativos de informação;

1.5.6. Clareza: as regras de gestão de riscos de segurança da informação e das comunicações devem ser precisas, concisas e de fácil entendimento;

1.5.7. Pessoalidade e utilidade do acesso aos ativos de informação;

1.5.8. Publicidade: dar transparência no trato da informação, observados os critérios legais;

1.5.9. Serão observados ainda, sem prejuízo dos demais, outros princípios constitucionais que regem a Administração Pública Federal – APF.

## 1.6. DIRETRIZES GERAIS

São diretrizes gerais da PGRSIC:

1.6.1. As diretrizes gerais do processo de GRSIC consideram, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do MI, além de estarem alinhadas à respectiva POSIC do MI;

1.6.2. As decisões estratégicas de SIC do MI devem observar os níveis de exposição aos riscos;

1.6.3. Deve ser adotada no MI a abordagem sistemática do processo de GRSIC, conforme preconizado na Norma Complementar 04/IN01/DSIC/GSI/PR e na Norma ABNT NBR ISO/IEC 27005:2011, com o objetivo de manter os riscos em níveis aceitáveis;

1.6.4. O processo de GRSIC do MI deverá ser definido pelas atividades de:

1.6.4.1. análise de contexto e identificação de requisitos de SIC;

1.6.4.2. análise e avaliação dos riscos;

1.6.4.3. definição do plano de tratamento dos riscos;

1.6.4.4. definição da estratégia de aceitação dos riscos;

1.6.4.5. implementação do plano de tratamento dos riscos, monitoração e análise crítica;

1.6.4.6. melhoria do processo de GRSIC;

1.6.5. O processo de GRSIC deve ser contínuo e deve estar alinhado ao modelo denominado PDCA (*Plan-Do-Check-Act*), conforme definido na Norma Complementar nº 02/IN01/DSIC/GSIPR, de modo a fomentar a sua melhoria contínua;

1.6.6. O processo de GRSIC deve ser aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações do MI e deverá produzir subsídios para suportar o Sistema de SIC e a Gestão de Continuidade de Negócios do MI;

1.6.7. Todos os riscos de segurança da informação e das comunicações devem ser identificados e tratados;

1.6.8. Todos os usuários são responsáveis pela identificação de riscos e devem prestar contas por gerenciar os riscos de suas atividades;

1.6.9. O MI deve difundir um sistema de cultura de risco, no qual procedimentos e sistemas de controle sejam disseminados em todas as áreas administrativas e operacionais, com total comprometimento da Alta Administração do MI;

1.6.10. Um sistema amplo de divulgação deve permear todo o MI de forma clara e objetiva;

1.6.11. Uma análise bem estruturada que avalie, identifique e reconheça o comprometimento de todos os usuários com o gerenciamento de riscos de segurança da informação e das comunicações é fundamental para o sucesso dessa iniciativa;

1.6.12. A adoção de uma linguagem padrão de GRSIC é essencial ao processo, possibilitando melhor entendimento entre as partes e um processo livre de interferências;

## 1.7. COMPETÊNCIAS E RESPONSABILIDADES

### 1.7.1. Compete ao DGE

1.7.1.1. Prover apoio aos setores do MI para o cumprimento da PGRSIC;

1.7.1.2. Auxiliar na aquisição de ferramentas de tecnologia de informação e demais recursos que viabilizem a implementação de PGRSIC no MI;

### 1.7.2. Compete ao Gestor de SIC

1.7.2.1. Coordenar a GRSIC no MI;

1.7.2.2. De acordo com as necessidades de cada setor do MI, indicar responsáveis pelo gerenciamento de atividades relacionadas à GRSIC, a quem serão conferidas, no mínimo, as seguintes atribuições:

1.7.2.2.1. Analisar, avaliar e tratar riscos;

1.7.2.2.2. Produzir relatórios de síntese, onde constem a análise dos resultados obtidos e a proposição de ajustes e de medidas preventivas e proativas ao Comitê de SIC.

### 1.7.3. Compete ao Comitê de SIC do MI

1.7.3.1. Deliberar quanto a decisões relacionadas à GRSIC, incluindo sanções na ocorrência de violação desta Política;

1.7.3.2. Revisar, divulgar e fazer cumprir esta Política no âmbito do MI;

1.7.3.3. Orientar e coordenar as atividades e projetos relativos à GRSIC do MI, promovendo programas educacionais e de conscientização em GRSIC;

1.7.3.4. Estabelecer e manter atualizados os normativos relativos à GRSIC no MI, em conjunto com as partes interessadas;

1.7.3.5. Definir modelos de relatórios para reporte de eventos e incidentes que comprometam a GRSIC no âmbito do MI;

1.7.3.6. Realizar auditorias periódicas para avaliar os níveis de conformidade desta Política e dos demais normativos de GRSIC no âmbito do MI;

1.7.3.7. Aprovar as diretrizes gerais e o processo de GRSIC, observada, dentre outras políticas, a POSIC vigente;

1.7.3.8. Implantar as diretrizes de GRSIC indicadas por esta Política.

**1.7.4. Compete aos Chefes de Setores do MI**

1.7.4.1. Garantir o cumprimento desta Política na esfera de responsabilidade do setor;

1.7.4.2. Detectar e encaminhar ao Comitê de SIC os casos de quebra da segurança da informação e das comunicações ocasionadas por riscos não identificados ou riscos que não foram tratados por usuários sob sua responsabilidade;

1.7.4.3. Realizar análise, avaliação e tratamento de riscos dos ativos de informação sob sua administração;

1.7.4.4. Contribuir para o processo de melhoria contínua da GRSIC monitorando e realizando análises críticas dos ativos do setor;

1.7.4.5. Comunicar às partes interessadas os riscos dos ativos de informação sob a administração do setor;

1.7.4.6. Reportar ao Comitê de SIC situações que comprometam a GRSIC.

**1.7.5. Compete aos Usuários da Informação**

1.7.5.1. Cumprir a PGRSIC do MI;

1.7.5.2. Reportar ao chefe imediato situações de riscos que comprometam a segurança das informações do MI.

## 1.8. SENSIBILIZAÇÃO, CONSCIENTIZAÇÃO E CAPACITAÇÃO

1.8.1. Todas as unidades do MI deverão manter um processo permanente de divulgação de suas normas e procedimentos para capacitar, conscientizar e sensibilizar seus usuários à correta conduta na utilização dos ativos do MI.

## 1.9. PENALIDADES

1.9.1. O não cumprimento das determinações da PGRSIC sujeita o infrator às penalidades previstas na legislação e nos regulamentos internos do MI;

1.9.2. O descumprimento das disposições constantes nesta Política e nas Normas Operacionais sobre Segurança da Informação e das Comunicações caracteriza infração

funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil;

1.9.3. O usuário que fizer uso de forma indevida ou não autorizada dos recursos de tecnologia da informação, bem como agir em desacordo com os termos desta Política, fica sujeito à aplicação das penalidades previstas na Lei 8.112/90 e na legislação pertinente;

1.9.4. Os casos omissos e as dúvidas surgidas na aplicação desta Política serão submetidos ao Comitê de SIC.

## 1.10. ATUALIZAÇÃO

1.10.1. Esta Política de GRSIC deve ser revisada e atualizada periodicamente no máximo a cada 3 (três) anos, sempre que forem observadas novas ameaças e vulnerabilidades, mudanças organizacionais e necessidades de atendimento a requisitos legais e regulatórios.

1.10.2. Esta Política de GRSIC deverá estar em conformidade com as Diretrizes do DGE, e será revisada e atualizada sempre que forem atualizadas ou aprovadas Normas relacionadas ao assunto pelo Ministério da Integração Nacional.

## 1.11. VIGÊNCIA

1.11.1. Esse documento entra em vigor na data de sua publicação.

## 1.12. DIVULGAÇÃO

1.12.1. Após a publicação desta Política de Gestão de Riscos de Segurança da Informação e das Comunicações, ela estará disponível permanentemente nos canais de comunicação interno e externo do MI e no D.O.U. a todos os usuários.

## 1.13. DISPOSIÇÕES FINAIS

1.13.1. Os casos omissos e as dúvidas com relação a esta POSIC serão submetidos ao Comitê de SIC do MI.