



**MINISTÉRIO DA INDÚSTRIA,
COMÉRCIO EXTERIOR E SERVIÇOS**
Comitê de Governança Digital

Número da Norma Complementar	Revisão	Emissão	Folha
01/Port. 04/CGD/MDIC	00	/DEZ/16	1/4

**Organização do Sistema de Gestão de Segurança da
Informação e Comunicação (SGSIC) do Ministério da
Indústria, Comércio Exterior e Serviços (MDIC)**

ORIGEM

Comitê de Governança Digital (CGD) do MDIC

REFERÊNCIA NORMATIVA E BIBLIOGRÁFICAS

NC 01/IN01/DSIC/GSIPR, de 15 de outubro de 2008.

NC 02/IN01/DSIC/GSIPR, de 14 de outubro de 2009.

PORTARIA 156/MDIC, de 31 maio de 2016.

PORTARIA 68/MPOG, de 7 de março de 2016.

DECRETO 8.638, de 15 de janeiro de 2016.

IN 01 GSI/PR, de 13 de junho de 2008.

CAMPO DE APLICAÇÃO

Esta Norma Complementar e seus anexos se aplicam no âmbito do MDIC

SUMÁRIO

- 1 Objetivo
- 2 Diretrizes
- 3 Vigência

INFORMAÇÕES ADICIONAIS

Não há

APROVAÇÃO

MARCOS JORGE DE LIMA
Presidente do Comitê de Governança Digital

Número da Norma Complementar	Revisão	Emissão	Folha
01/Port. 04/CGD/MDIC	00	/DEZ/16	2/4

1 OBJETIVO

O Sistema de Gestão de Segurança da Informação e Comunicação (SGSIC) é um conjunto de processos e procedimentos, baseado em normas e na legislação vigente, que uma organização deve implementar para prover segurança no uso de seus ativos tecnológicos de modo a preservá-los quanto aos aspectos de disponibilidade, integridade, confidencialidade e autenticidade, independentemente do meio em que se encontram. Nesse contexto, este documento estabelece premissas e responsabilidades para implementação e estruturação do SGSIC, que terá como metodologia de gestão a melhoria contínua com base no ciclo PDCA.

2 DIRETRIZES

2.1 Premissas

2.1.1 Compõem o SGSIC:

- a) Em nível estratégico, a Política de Segurança da Informação e Comunicações (POSIC) do MDIC;
- b) Em nível tático, Normas Complementares à POSIC; e
- c) Em nível operacional, Procedimentos de Segurança.

2.1.2 A estrutura orgânica do SGSIC é composta por:

- a) Comitê de Governança Digital (CGD);
- b) Comitê de Segurança da Informação e Comunicações (CSIC);
- c) Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR); e
- d) Gestor de Segurança da Informação e Comunicações.

2.1.3 É de responsabilidade de todos os integrantes da estrutura orgânica do SGSIC zelar pelo cumprimento da POSIC e das Normas Complementares a ela, bem como dar publicidade e promover a cultura de Segurança da Informação e Comunicações (SIC).

2.2 Responsabilidades

2.2.1 **O Comitê de Governança Digital** foi instituído pela Portaria GM nº 156, de 31 de maio de 2016, e é responsável por avaliar e deliberar sobre as políticas de segurança da informação e comunicações e privacidade dos usuários e dos cidadãos cadastrados nos serviços digitais do Ministério, além de aprovar a POSIC, ou instrumento equivalente, e demais políticas relacionadas ao tema, em alinhamento à Estratégia de Governança Digital do Governo Federal.

2.2.2 São competências e responsabilidades do CGD no âmbito da segurança da informação e comunicação:

- a) Nomear Gestor de Segurança da Informação e Comunicações;
- b) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicação;
- c) Avaliar as ocorrências encaminhadas pela ETIR;
- d) Propor alterações na Política de Segurança da Informação e Comunicação;

Número da Norma Complementar	Revisão	Emissão	Folha
01/Port. 04/CGD/MDIC	00	/DEZ/16	3/4

- e) Propor normas e procedimentos relativos à segurança da informação e comunicação no âmbito do MDIC;
- f) Aprovar as alterações da POSIC e suas Normas Complementares; e
- g) Aprovar as revisões periódicas da POSIC e suas Normas Complementares.

2.2.3 O Gestor de Segurança da Informação e Comunicação (GSIC) e seu substituto serão servidores públicos efetivos designados pelo CGD.

2.2.4 São competências e responsabilidades do GSIC no âmbito da segurança da informação e comunicação:

- a) Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
- b) Propor recursos necessários às ações de segurança da informação e comunicação;
- c) Coordenar o Comitê de Segurança da Informação e Comunicação e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
- d) Realizar estudos quanto às novas tecnologias de Segurança da Informação e Comunicação, a viabilidade ou necessidade de implantação ou utilização no âmbito do MDIC;
- e) Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI-PR) para o trato de assuntos relativos à segurança da informação e comunicação;
- f) Propor normas e procedimentos relativos à segurança da informação e comunicação no âmbito do MDIC; e
- g) Propor ações de auditoria de Segurança da Informação e Comunicações.

2.2.5 O Comitê de Segurança da Informação e Comunicações será composto, no mínimo, por um representante de cada área da CGTI.

2.2.6 Compete ao CSIC:

- a) Zelar pelo funcionamento do Sistema de Gestão de Segurança da Informação e Comunicação;
- b) Assessorar na implementação das ações de segurança da informação e comunicação;
- c) Sugerir ações que visem à proteção dos ativos de informação;
- d) Realizar periodicamente análise crítica e sugerir alterações da POSIC e de suas Normas Complementares;
- e) Monitorar as principais mudanças e configurações dos ativos de informação; e
- f) Propor ferramentas e procedimentos para subsidiar a atuação da ETIR, visando a disponibilidade, integridade, confidencialidade e autenticidade.

2.2.7 A Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais (ETIR) visa cumprir os procedimentos de tratamento e resposta a incidentes de acordo com o estabelecido em Norma Complementar específica.

2.2.8 São ainda responsáveis por ações de Segurança da Informação e Comunicações:

Número da Norma Complementar	Revisão	Emissão	Folha
01/Port. 04/CGD/MDIC	00	/DEZ/16	4/4

- a) **A área de Tecnologia da Informação e Comunicação:** deve executar atividades pertinentes à segurança lógica do ambiente e dos recursos de processamento da informação;
- b) **A área de Recursos Logísticos e Administração Predial:** deve executar atividades pertinentes à segurança física e patrimonial do ambiente e dos recursos de processamento da informação;
- c) **A área de Gestão de Pessoas:** deve executar ações de treinamento e desenvolvimento referentes à segurança da informação e comunicação, bem como aquelas referentes a gestão de pessoas que interajam com os recursos de processamento da informação; e
- d) **A área de Comunicação Social:** deve executar atividades relacionadas à comunicação institucional, divulgando e disseminando as orientações emanadas pela Política de Segurança da Informação e Comunicação do MDIC.

3 VIGÊNCIA

Esta Norma entra em vigor na data da sua publicação.