



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

Número da Norma Complementar	Revisão	Emissão	Folha
00/IN01/DSIC/GSIPR	00	DD/MM/14	1/5

**PADRÕES MÍNIMOS DE SEGURANÇA DA INFORMAÇÃO E
COMUNICAÇÕES PARA OS SISTEMAS ESTRUTURANTES DA
ADMINISTRAÇÃO PÚBLICA FEDERAL**

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

Decreto-Lei nº 200, de 25 de fevereiro de 1967

Decreto nº 3.505, de 13 de junho de 2000

Decreto nº 8.135, de 04 de novembro de 2013

Lei nº 12.527, de 18 de novembro de 2011

Decreto nº 7.845, de 14 de novembro de 2012

Instrução Normativa GSI 01 de 13 de junho de 2008

Instrução Normativa SLTI/MP nº 4 de 12 de novembro de 2010

Normas Complementares 01, 02, 04, 06, 07, 10, 13, 14 e 16 da IN01/DSIC/GSIPR de 13 de outubro de 2008

CAMPO DE APLICAÇÃO

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

SUMÁRIO

1. Objetivo
2. Fundamento Legal da Norma Complementar
3. Conceitos e Definições
4. Princípios, Diretrizes e Procedimentos
5. Responsabilidades
6. Vigência

INFORMAÇÕES ADICIONAIS

Não há

APROVAÇÃO

RAPHAEL MANDARINO JUNIOR

Diretor do Departamento de Segurança da Informação e Comunicações

Número da Norma Complementar	Revisão	Emissão	Folha
00/IN01/DSIC/GSIPR	00	DD/MM/14	2/5

1 OBJETIVO

Estabelecer padrões mínimos para a segurança da informação e comunicações dos sistemas estruturantes nos órgãos e entidades 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 CONCEITOS E DEFINIÇÕES

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

3.1 **Ativos de informação:** os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

3.2 **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.

3.3 **Custodiante:** aquele que, de alguma forma e total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema estruturante – ou de ativos de informação que compõem um estruturante – que não lhe pertence, mas que está sob sua custódia.

3.4 **Gestão de Riscos de Segurança da Informação e Comunicações:** conjunto de processos que permite identificar e implementar controles e 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.

3.5 **Sistema de Proteção Física:** sistema composto por pessoas, equipamentos e procedimentos para a proteção de ativos contra danos, roubo, sabotagem e outros prejuízos causados por ações humanas não autorizadas, conforme gestão da segurança física e ambiental.

3.6 **Sistema Estruturante:** sistema com suporte de tecnologia da informação fundamental e imprescindível para planejamento, coordenação, execução, descentralização, delegação de competência, controle ou auditoria das ações do Estado, além de outras atividades auxiliares, desde que comum a dois ou mais órgãos da Administração e que necessitem de coordenação central.

3.7 **Gestão Unificada de Identidades e Acessos:** conjunto de processos e de plataforma de tecnologia da informação que dá suporte à centralização, administração e gestão de toda a base de usuários dos sistemas de informação da APF e de seus respectivos perfis de acesso.

3.8 **Trilha de Auditoria:** registro ou conjunto de registros gravados em arquivos de *log* ou outro tipo de documento ou mídia, que possam indicar, de forma cronológica e inequívoca, o autor e a ação realizada em determinada operação, procedimento ou evento.

3.9 **Autenticação de multifatores:** utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema. Os fatores de autenticação se dividem em: algo que o usuário

Número da Norma Complementar	Revisão	Emissão	Folha
00/IN01/DSIC/GSIPR	00	DD/MM/14	3/5

sabe (senhas, frases de segurança, PIN, dentre outros); algo que o usuário possui (certificado digital, *tokens*, códigos enviados por SMS e similares) ou algo que o usuário é (aferrível por meios biométricos, tais como digitais, padrões de retina, reconhecimento facial, dentre outros).

4 PRINCÍPIOS, DIRETRIZES E PROCEDIMENTOS

Os padrões de segurança dos sistemas estruturantes deverão incorporar, gradativamente, controles de segurança da informação e comunicações (SIC), no mínimo, no que tange aos seguintes aspectos:

4.1 PLANEJAMENTO, CONCEPÇÃO E MANUTENÇÃO DO SISTEMA

4.1.1 As demandas de planejamento que resultem em sistemas estruturantes deverão seguir as diretrizes para a gestão de continuidade de negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, conforme Norma Complementar nº 6 à IN01/DSIC/GSIPR.

4.1.2 A integração, a fusão ou a ampliação de sistemas legados que ensejarem novos ou reformulados sistemas estruturantes deverá observar as diretrizes para a Gestão de Mudanças, nos aspectos relativos à Segurança da Informação e Comunicações, recomendadas na Norma Complementar nº 13 à IN01/DSIC/GSIPR.

4.1.3 O desenvolvimento e obtenção de *software* para sistema estruturante deverá observar as diretrizes recomendadas na Norma Complementar nº 16 à IN01/DSIC/GSIPR.

4.1.4 Os sistemas estruturantes deverão atender aos padrões de interoperabilidade estabelecidos pela e-PING/SLTI/MP.

4.1.5 As contratações de soluções de tecnologia da informação decorrentes de projetos de implementação ou manutenção de sistemas estruturantes deverão observar as fases preconizadas pela Instrução Normativa nº 4 da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão, salvo as disposições contrárias, conforme legislação em vigor.

4.1.6 Os instrumentos contratuais celebrados entre a APF e prestadores de serviço, em decorrência das contratações de soluções de tecnologia da informação para projetos de implementação ou manutenção de sistemas estruturantes, deverão conter cláusulas que viabilizem a realização de auditorias multidisciplinares e periódicas nos aspectos de SIC de tais prestadores.

4.1.7 Os sistemas estruturantes deverão utilizar tecnologias seguras de *hardware* e de *software* compatíveis com o sigilo das informações por eles manipuladas, conforme legislação em vigor.

4.1.7.1 Na medida do possível, os sistemas estruturantes devem reduzir, gradualmente, sua dependência externa em relação a ativos de informação constituídos por arquiteturas proprietárias, devendo optar por aqueles de arquitetura aberta.

4.2 INFRAESTRUTURA

4.2.1 Os dispositivos de armazenamento, recuperação e contingência de dados que suportam, total ou parcialmente, sistemas estruturantes deverão estar fisicamente localizados em dependências de um ou mais órgãos ou entidades públicos da administração pública federal, dentro do território nacional, conforme legislação em vigor.

Número da Norma Complementar	Revisão	Emissão	Folha
00/IN01/DSIC/GSIPR	00	DD/MM/14	4/5

4.2.2 Na medida do possível, os dispositivos de armazenamento, recuperação, processamento de dados e interconectividade de rede deverão priorizar modelos de fabricantes nacionais, conforme legislação em vigor.

4.2.3 As soluções de infraestrutura em nuvem para sistemas estruturantes deverão adotar somente os modelos de implementação de Nuvem Própria ou Nuvem Comunitária, em todos os modelos de serviços, conforme Norma Complementar nº 14 à IN01/DSIC/GSIPR.

4.2.4 As infraestruturas de rede e telecomunicações utilizadas pelos sistemas estruturantes deverão ser fornecidas por órgãos ou entidades da administração pública federal, conforme dispositivos legais em vigor.

4.2.5 As instalações de infraestrutura computacional, de armazenamento e recuperação de dados, de rede e de telecomunicações utilizadas, total ou parcialmente, por sistema estruturante deverão ser planejadas, operacionalizadas e continuamente monitoradas por processo formal de Gestão de Riscos de Segurança da Informação e Comunicações, observando-se, principalmente:

4.2.5.1 Sistemas de Proteção Física para mitigar o risco de acesso não autorizado;

4.2.5.2 Sistemas alternativo de provisão de energia elétrica;

4.2.5.3 Proteção contra descargas elétricas e atmosféricas;

4.2.5.4 Planos e sistemas de proteção contra incêndio e outros sinistros;

4.2.5.5 Eventual sítio alternativo em outra localidade, para a disponibilidade do sistema em caso de sinistro do sítio principal.

4.2.5.6 Utilização de infraestrutura de redes e telecomunicações seguras.

4.3 CONTROLE DE ACESSO E IDENTIDADES

4.3.1 Todo acesso ao sistema estruturante deverá observar as diretrizes recomendadas na Norma Complementar nº 7 à IN01/DSIC/GSIPR.

4.3.2 O acesso lógico ao sistema estruturante deverá ser integrado à gestão unificada de identidades e acessos da APF, quando disponível, e deverá empregar:

4.3.2.1 método de autenticação de usuário com mais de um fator – autenticação de multifatores – sempre que possível;

4.3.2.2 método de autenticação de usuário com certificação digital, no mínimo, no caso dos gestores, operadores administrativos do sistema estruturante e perfis críticos de acesso, conforme legislação em vigor.

4.3.3 Os sistemas estruturantes devem conter um conjunto de processos de negócio e de mecanismos lógicos e físicos capazes de viabilizar, quando necessário, trilhas de auditoria que darão apoio ao controle de Acesso Físico e Lógico, no tocante ao uso e manutenção de suas identidades digitais, conforme Norma Complementar nº 7 à IN01/DSIC/GSIPR.

4.3.3.1 Os estruturantes que tratam informações com algum grau de sigilo e aqueles relacionados à liberação ou manipulação de recursos públicos devem implementar trilhas de auditoria, conforme legislação em vigor.

Número da Norma Complementar	Revisão	Emissão	Folha
00/IN01/DSIC/GSIPR	00	DD/MM/14	5/5

4.4 TRATAMENTO DE INCIDENTES

4.4.1 O órgão ou unidade responsável pelo sistema estruturante deverá possuir Equipe de Tratamento e resposta a Incidentes em Redes Computacionais, apta a identificar e tratar os possíveis incidentes que comprometam a segurança da informação e comunicações relacionados ao estruturante, devendo o órgão viabilizar capacitação dessa equipe e, quando aplicável, ferramentas para sua atuação, conforme Norma Complementar n. 5 à IN01/DSIC/GSIPR.

4.4.2 Os incidentes de SIC identificados como ataques deverão ser submetidos ao CTIR.Gov, conforme legislação em vigor.

4.5 POLÍTICA E CONFORMIDADE

4.5.1 Os órgãos e entidades da APF gestores dos estruturantes devem estabelecer formalmente diretrizes, papéis, responsabilidades e controles nos casos em que os sistemas são delegados a um custodiante.

4.5.2 Os sistemas estruturantes devem possuir política ou normativo específico que disciplina seu uso, seus controles e perfis de acesso, bem como responsabilidades decorrentes de sua má utilização, conforme legislação em vigor.

4.5.2.1 Os normativos de que trata o caput devem ser revisados e ajustados periodicamente.

5 RESPONSABILIDADES

5.1 Caberá aos órgãos e entidades da APF, no âmbito de suas competências, cumprir e fazer cumprir as determinações contidas nesta norma, inclusive as possíveis cláusulas contratuais com eventuais fornecedores, sob pena de responsabilidade;

6 VIGÊNCIA

6.1 Esta norma entra em vigor na data de sua publicação.