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

PADRÕES MÍNIMOS DE SEGURANÇA PARA OS SISTEMAS ESTRUTURANTES DE TECNOLOGIA DA INFORMAÇÃO DA ADMINISTRAÇÃO PÚBLICA

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 4.553, de 27 de dezembro de 2002~~
Instrução Normativa GSI 01 de 13 de junho de 2008
Instrução Normativa SLTI/MP nº 4 de 12 de novembro de 2010
Norma Complementar 01/DSIC/GSIPR de 13 de outubro de 2008
Norma Complementar 02/DSIC/GSIPR de 13 de outubro de 2008
Norma Complementar 04/DSIC/GSIPR de 15 de fevereiro de 2013
Norma Complementar 06/DSIC/GSIPR de 11 de novembro de 2009
Norma Complementar 07/DSIC/GSIPR de 06 de maio de 2010
Norma Complementar 13/DSIC/GSIPR de 30 de janeiro de 2012
Norma Complementar 14/DSIC/GSIPR de 30 de janeiro de 2012

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

Estabelecer padrões mínimos para a segurança da informação e comunicações dos sistemas estruturantes nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF).

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 RESPONSABILIDADES

3.1 Caberá aos órgãos e entidades da APF, no âmbito de suas competências, atender os padrões de segurança da informação e comunicações para os sistemas estruturantes de Tecnologia da Informação, em conformidade com as orientações contidas nesta norma, sob pena de responsabilidade;

3.2 Os órgãos responsáveis pelos sistemas estruturantes deverão observar os princípios e diretrizes do processo de Gestão de Riscos de Segurança da Informação e Comunicações, conforme Norma Complementar n. 04 à IN01/DSIC/GSIPR;

4 TERMOS E DEFINIÇÕES

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

Acrescentar definições

4.x - **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.

4.x - **Gestão de Riscos de Segurança da Informação e Comunicações**: 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

4.x - **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.

4.x - **Sistema Estruturante**: sistema com suporte de tecnologia da informação organizado para planejamento, coordenação, descentralização, delegação de competência ou controle de atividades de pessoal, orçamento, estatística, administração financeira, contabilidade e auditoria, ou serviços gerais, além de outras atividades auxiliares, desde que comum a dois ou mais órgãos da Administração e que necessitem de coordenação central.

Sistema de Proteção Física: definir

Trilhas de Auditoria:

5 PLANEJAMENTO DO SISTEMA

5.1 - 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~~, de 6 de maio de 2010~~.

~~., de 12 de novembro de 2010s pela Instrução Normativa nº 4 da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestãooas fases preconizad, no que couber, basear-se n5.2 - As contratações de soluções de tecnologia da informação decorrentes de projetos de implementação de sistemas estruturantes deverão~~

5.2~~3~~ A integração, fusão ou ampliação de sistemas legados que ensejarem novos 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~~, de 30 de janeiro de 2012~~.

~~5.4 Interoperabilidade~~

5.3~~5~~ O desenvolvimento e obtenção de *software* para sistema estruturante deverá observar as diretrizes recomendadas na Norma Complementar nº 16 à IN01/DSIC/GSIPR~~, de 21 de novembro de 2012~~.

5.4 Os sistemas estruturantes deverão atender aos padrões de interoperabilidade estabelecidos pela e-PING/SLTI/MP (sistemas legados?)

5.5 - As contratações de soluções de tecnologia da informação decorrentes de projetos de implementação 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.

5.6 – Os órgãos e entidades da APF deverão, gradativamente, reduzir a dependência externa em relação aos ativos de informação vinculados à Segurança da Informação. (como prover meios para tal?)

5.7 – Normativos?

6 INFRAESTRUTURA

6.1 Os dispositivos de armazenamento, ~~e~~ 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 dentro do território nacional.

6.2 A infraestrutura de suporte ao sistema estruturante deverá possuir, no mínimo, um sítio alternativo em outra localidade para a disponibilidade do sistema em caso de sinistro do sítio principal.

6.2 ~~A infraestrutura computacional do sistema estruturante para o processamento principal dos dados, total ou parcial, deverá estar fisicamente localizada em dependências de um ou mais órgãos públicos dentro do território nacional, exceto o equipamento de processamento computacional para o acesso de clientes ao sistema, conforme a arquitetura utilizada.~~

6.3 Os dispositivos de armazenamento, recuperação, processamento de dados e interconectividade de rede, quando possível, deverão priorizar modelos de fabricantes nacionais, conforme legislação em vigor (fecha mercado nas licitações. Fabricantes nacionais muitas vezes nem possuem equipamentos com as características necessárias)~~.~~

6.4 As soluções de infraestrutura em nuvem para sistemas estruturantes deverão adotar~~adotará~~ 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~~, de 30 de janeiro de 2012~~.

6.5 As infraestruturas de rede e telecomunicações utilizadas pelos sistemas estruturantes~~, quando possível,~~ deverão priorizar, quando possível, sistemas próprios da Administração Pública, conforme legislação em vigor.

6.6 Os sistemas estruturantes deverão utilizar infraestruturas de rede e telecomunicações seguras, conforme Gestão de Riscos de Segurança da Informação e Comunicações aplicada ao sistema.

6.7 As instalações de infraestrutura computacional, de armazenamento e recuperação de dados, de rede~~,~~ e de telecomunicações~~,~~ utilizadas, total ou parcialmente, por sistema estruturante deverão possuir:

~~-~~6.7.1 ~~-~~ Sistema de Proteção Física para mitigar o risco de acesso não autorizado;~~.~~

6.7.2 – Sistema alternativo de provisão de energia elétrica;

6.7.3 – Proteção contra descargas elérticas e atmosféricas;

6.7.4 – Planos e sistemas de proteção contra incêndio e outros sinistros;

~~6.8 As instalações de infraestrutura computacional, de armazenamento e recuperação de dados, de rede, e de telecomunicações, utilizadas, total ou parcialmente, por sistema estruturante deverão possuir, no mínimo, sistema alternativo de provisão de energia elétrica, proteção contra descargas elétricas atmosféricas, bem como, planos e sistemas de proteção contra incêndio e outros sinistros.~~

~~6.9 A infraestrutura de suporte ao sistema estruturante deverá possuir, no mínimo, um sítio alternativo em outra localidade para a disponibilidade do sistema em caso de sinistro do sítio principal.~~

7 ACESSO

7.1 Todo acesso ao sistema estruturante deverá observar as diretrizes recomendadas na Norma Complementar nº 7 à IN01/DSIC/GSIPR~~, de 6 de maio de 2010~~.

7.2 O acesso lógico ao sistema estruturante deverá empregar, quando possível, método de autenticação de usuário com mais de um fator – autenticação de multifatores.

7.3 O acesso lógico ao sistema estruturante deverá empregar método de autenticação de usuário com certificação digital, ~~conforme legislação em vigor~~, no mínimo, no caso dos operadores administrativos do sistema estruturante e perfis críticos de acesso, conforme legislação em vigor~~.~~

7.4 Os sistemas estruturantes que utilizem redes de dados no padrão TCP/IP (*Transmission Control Protocol - Internet Protocol*) deverão, no mínimo, utilizar protocolos de segurança na camada de aplicação, permitindo que os dados sejam transmitidos por meio de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente por meio de certificados digitais.

7.5 – Os sistemas estruturantes devem conter um conjunto de processos de negócio e de mecanismos lógicos e físicos, quando necessários, capazes de viabilizar trilhas de auditoria que darão apoio ao controle de Acesso Físico e Lógico, no tocante ~~infraestrutura com suporte para criação, manutenção,~~ ao uso e manutenção de suas ~~de~~ identidades digitais ~~e trilhas de auditoria que darão apoio ao Controle de Acesso Físico e Lógico~~, conforme :
~~(~~NC 07/IN01/DSIC/GSIPR~~)~~

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

8 TRATAMENTO DE INCIDENTES

8.1 – 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 relacionados à Segurança da Informação e Comunicações relacionados ao estruturante, conforme Norma Complementar n. 5 à IN 01/DSIC/GSIPR.

8.2 – Os incidentes de SIC deverão ser submetidos ao CTIR.Gov, conforme legislação em vigor.

9 ~~VIGÊNCIA~~

Esta norma entra em vigor na data de sua publicação.