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 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.

3.2 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.

3.3 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 conhece (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 (aferível por meios biométricos, tais como digitais, padrões de retina, reconhecimento facial, dentre outros).

3.4 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.

3.5 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.

3.6 Modelo de Implementação de Nuvem Própria: solução compartilhada de recursos computacionais configuráveis cuja infraestrutura da nuvem pertence apenas a uma organização e suas subsidiárias.

3.7 Modelo de Implementação de Nuvem Comunitária: solução compartilhada de recursos computacionais configuráveis cuja infraestrutura da nuvem é compartilhada entre diversas organizações que possuem necessidades comuns, tais como, missão, valores, requisitos de segurança, políticas, requisitos legais, entre outras.

3.8 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.

3.9 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.

3.10 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.

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, concepção e manutenção de sistemas estruturantes deverão seguir processo formal de Gestão de Riscos de Segurança da Informação e Comunicações.

4.1.2 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/GSI/PR.

4.1.3 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.

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

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

4.1.6 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.

4.1.7 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 garantam a realização de auditorias nos aspectos de Segurança da Informação e Comunicações.

4.1.8 Preferencialmente, os sistemas estruturantes devem optar por ativos de informação constituídos por arquiteturas que permitam auditar seus respectivos projetos e códigos, conforme legislação em vigor.

4.2 Infraestrutura

4.2.1 Os dispositivos de armazenamento 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.

4.2.2 Os dispositivos de armazenamento, recuperação, processamento de dados e interconectividade de rede poderão adotar preferência por 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 de Nuvem Comunitária, em todos os modelos de serviços, conforme Norma Complementar nº 14 à IN01/DSIC/GSI/PR, desde que restritas às infraestruturas de órgãos ou entidades da administração pública federal.

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:

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

b) Sistema alternativo de provisão de energia elétrica;

c) Proteção contra descargas elétricas e atmosféricas;

d) Planos e sistemas de proteção contra incêndio e outros sinistros;

e) Sítio alternativo que garanta a disponibilidade do sistema em caso de sinistro.

f) 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/GSI/PR.

4.3.2 O acesso lógico ao sistema estruturante deverá empregar os seguintes métodos de autenticação de usuário:

4.3.2.1 Autenticação de usuário com mais de um fator - autenticação de múltiplos fatores - sempre que possível; e

4.3.2.2 N o mínimo, autenticação com certificação digital para gestores, operadores administrativos 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 aos controles de acesso, principalmente, no tocante ao uso e manutenção das identidades digitais, conforme Norma Complementar nº 7 à IN01/DSIC/GSI/PR.

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

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 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/GSI/PR.

4.4.2 Os incidentes de SIC identificados deverão ser informados 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

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

Esta norma entra em vigor na data de sua publicação.

PORTARIA Nº 25, DE 15 DE JULHO DE 2014

Homologa a Norma Complementar nº 20/IN01/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 de suas atribuições e tendo em vista o disposto no art. 6º e no art. 7º do Decreto nº 3.505, de 13 de junho de 2000, com nova redação dada pelo Decreto nº 8.097, de 4 de setembro de 2013, resolve:

Art. 1º Fica homologada a Norma Complementar nº 20/IN01/DSIC/GSIPR que estabelece Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

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

JOSÉ ELITO CARVALHO SIQUEIRA

DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

E COMUNICAÇÕES PARA INSTITUIÇÃO DO PROCESSO

DE TRATAMENTO DA INFORMAÇÃO NOS ÓRGÃOS

E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

Lei nº 1.079, de 10 de abril de 1950.
Lei nº 8.112, de 11 de dezembro de 1990.
Lei nº 8.159, de 08 de janeiro de 2001.
Lei nº 12.527, de 18 de novembro de 2011.
Decreto nº 2848, de 07 de dezembro de 1940.
Decreto nº 3.505, de 13 de junho de 2000.
Decreto nº 4.915, de 12 de dezembro de 2003.
Decreto nº 7724, de 16 de maio de 2012.
Decreto nº 7845, de 14 de novembro de 2012.
Decreto nº 8135, de 04 de novembro de 2013.
Resolução nº 07/Conarq, de 20 de maio de 1997.
Resolução nº 14/Conarq, de 24 de outubro de 2001.
Portaria nº 03/SLTI/MP, de 16 de maio de 2003.
Portaria Normativa nº 05/SLTI/MP, de 19 de dezembro de 2002.
Instrução Normativa nº 01/DSIC/GSI/PR, de 13 de junho de 2008 e suas Normas Complementares.
Instrução Normativa nº 02/DSIC/GSI/PR, de 05 de fevereiro de 2013.
ABNT NBR ISO/IEC 27001:2013.
ABNT NBR ISO/IEC 27002:2013.
ABNT NBR 16167:2013.

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 diretrizes de Segurança da Informação e Comunicações para instituição do processo de tratamento da informação, envolvendo todas as etapas do ciclo de vida da informação, no âmbito da Administração Pública Federal, direta e indireta.

2 CONSIDERAÇÕES INICIAIS

Os órgãos e entidades da Administração Pública Federal (APF) produzem e tratam informações diariamente na rotina de trabalho de seus agentes públicos, ocupando relevância fundamental para a gestão da máquina pública e o processo de tomada de decisões quanto às políticas públicas federais.

Neste sentido, a presente norma dispõe acerca de diretrizes a serem cumpridas no âmbito órgãos e entidades da APF quanto ao adequado tratamento da informação durante as fases do seu do ciclo de vida.

Esta norma configura instrumento complementar as políticas, procedimentos e regras regulamentados por atos normativos que norteiam o tratamento da informação nos órgãos e entidades da APF. Por essa razão, ressalta-se a importância da observação, por parte dos agentes públicos, dos dispositivos estabelecidos na legislação relativa a temas como Segurança da Informação e Comunicações (SIC), gestão documental e arquivística, gestão da informação, acesso à informação, e sigilo da informação.

3 CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:

Agente Público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da APF.

Ciclo de vida da informação: ciclo formado pelas fases da Produção e Recepção; Registro e Armazenamento; Uso e Disseminação; e Destinação.

Documento: unidade de registro de informações, qualquer que seja o suporte ou formato.

Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

Informação classificada: informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, a qual é classificada como ultrassecreta, secreta ou reservada.

Metadados: dados que descrevem os dados, isto é, são informações úteis para identificar, localizar, compreender e gerenciar os dados.

Tratamento da informação: conjunto de ações referentes às fases do ciclo de vida da informação.

4 DIRETRIZES GERAIS

4.1 Toda informação institucional dos órgãos e entidades da APF em qualquer suporte, materiais, áreas, comunicações e sistemas de informação institucionais, é patrimônio do Estado brasileiro e deve ser tratada segundo as diretrizes descritas nesta Norma Complementar, nos termos da legislação pertinente em vigência.

4.2 O tratamento das informações ao longo de seu ciclo de vida deverá ser realizado de modo ético e responsável pelos agentes públicos dos órgãos e entidades da APF e com respeito à legislação vigente.

4.3 O tratamento da informação deverá ser feito conforme atos normativos de Segurança da Informação e Comunicações (SIC), assegurando-se os requisitos da disponibilidade, da integridade, da confidencialidade e da autenticidade da informação em todo seu ciclo de vida.

4.4 As informações institucionais dos órgãos e entidades da APF deverão ser tratadas visando-se as suas funções administrativas, informativas, probatórias e comunicativas, e considerados os princípios de acesso a informação dispostos pela Lei 12.527/2011.

4.5 É dever do agente público salvaguardar a informação classificada, sigilosa ou pessoal, bem como assegurar a publicidade da informação de caráter ostensivo, utilizando-as, exclusivamente, para o exercício das atribuições de cargo, emprego ou função pública, sob pena de responsabilização administrativa, civil e penal.

4.6 As medidas e os procedimentos relacionados ao tratamento da informação a ser realizado com apoio de empresas terceirizadas, em qualquer fase do ciclo de vida da informação, deverão ser estabelecidos contratualmente para que se assegure o cumprimento das diretrizes previstas nesta norma, bem como em legislações vigentes.

4.7 Os órgãos e entidades da APF devem promover ações para conscientização dos agentes públicos visando à disseminação das diretrizes de tratamento da informação.

5 CICLO DE VIDA DA INFORMAÇÃO

O tratamento da informação abrange as políticas, os processos, as práticas e os instrumentos utilizados pelos órgãos e entidades da APF para lidar com a informação ao longo de cada fase de seu ciclo de vida, contemplando o conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Para efeito desta norma, as ações referidas estão agrupadas nas seguintes fases, conforme Anexo A:

5.1 Produção e Recepção: refere-se ao estágio em que as informações são produzidas ou recebidas pelos agentes públicos, independentemente de seu formato ou suporte.

5.2 Registro e Armazenamento: diz respeito à fase em que as informações são registradas e armazenadas em quaisquer suportes ou formatos.

5.3 Uso e Disseminação: trata-se do estágio em que as informações estão sendo utilizadas e compartilhadas pelos órgãos e entidade da APF, envolvendo ações como o seu uso, transporte, transmissão e divulgação.

5.4 Destinação: refere-se ao estágio final do ciclo de vida da informação, no qual devem ser tomadas as medidas necessárias à sua destinação, tais como guarda permanente ou eliminação.

6 DIRETRIZES ESPECÍFICAS

6.1 Produção e Recepção

Os principais aspectos a serem observados pelos órgãos e entidades da APF na fase da produção ou recepção são:

6.1.1 Os processos de produção e recepção das informações deverão ser planejados e implementados considerando-se:

a) os interesses da APF;

b) o período previsto para a retenção das informações; e

c) os custos com recursos materiais, financeiros e pessoas.

6.1.2 A produção e a recepção de informações deverão ser feitas de modo que seu registro possa estar disponível e acessível a todos os agentes públicos que delas necessitarem para o desempenho de suas atribuições.

6.1.3 Com vistas a garantir as condições essenciais ao aprofundamento da democratização do acesso a informação no âmbito interno e externo aos órgãos e entidades da APF, deve-se priorizar a produção de informações em linguagem clara e precisa independentemente de seu formato ou suporte.

6.1.4 Os órgãos e entidades da APF deverão garantir que a produção e a recepção de informações sejam feitas com a devida proteção das informações pessoais.

6.1.5 Na fase da produção e recepção de informações, os órgãos e entidades da APF deverão verificar se as informações por eles produzidas ou custodiadas se enquadram em quaisquer hipóteses de sigilo especificadas na Lei 12.527/2011 ou em legislações específicas - tais como aquelas referentes aos sigilos legal, fiscal e bancário, ao segredo industrial ou de justiça (conforme Anexo B) -, a fim de adotar as medidas cabíveis quanto ao seu tratamento.

6.1.6 Nas reuniões em que serão produzidas informações sigilosas, deverão ser adotados controles de acesso ao ambiente, documentos, anotações, mídias e demais recursos utilizados.

6.1.7 Quando a produção de informação sigilosa exigir impressão em tipografias, impressoras, oficinas gráficas ou similares, a operação deverá ser acompanhada por pessoa credenciada, responsável pela execução das medidas de salvaguarda necessárias à garantia do sigilo durante todo o processo.

6.1.8 Recomenda-se que, durante a produção e a recepção de informações, sejam identificados os metadados necessários para a gestão da informação nos órgãos e entidades da APF.

6.2 Registro e Armazenamento

Os aspectos principais a serem observados pelos órgãos e entidades da APF na fase do registro e armazenamento são:

6.2.1 A seleção, dentre as opções de registro e armazenamento de informações, deverá considerar:

a) as características físicas do suporte e do ambiente;

b) o volume e estimativa de crescimento;

c) o período previsto para a retenção da informação;

d) a proteção contra acesso não autorizado;

e) as eventuais necessidades de classificação e preservação das informações conforme atos normativos correlatos;

f) as perdas por destruição, furto ou sinistro;

g) a frequência de uso;

h) os custos relativos ao seu armazenamento.

6.2.2 É dever do agente público a manutenção dos registros que tenham servido de fundamento ao ato administrativo.

6.2.3 Para o registro de seus documentos arquivísticos, os órgãos e entidades da APF devem observar as legislações pertinentes que tratam dos procedimentos gerais para utilização de protocolo na APF.

6.2.4 Na fase do registro e armazenamento das informações, os órgãos e entidades da APF deverão avaliar eventuais necessidades de indexação, catalogação, classificação e marcação das informações, conforme arcabouço legal existente e orientações adicionais internas que se fizerem necessárias.

6.2.5 Os órgãos e entidades da APF deverão priorizar a adoção de formatos abertos e não proprietários, sempre que possível, para preservar as informações digitais e permitir seu amplo acesso, conforme padrões de interoperabilidade do Governo Eletrônico.

6.2.6 Os órgãos e entidades da APF deverão adotar os procedimentos de controle de acesso necessários à segurança dos registros e armazenamento das informações.

6.2.7 Os órgãos e entidades da APF deverão manter controle sobre eventuais cópias de registros de informações, zelando também por seu adequado armazenamento, garantindo-se a rastreabilidade das cópias de segurança e restauração das informações por meio da manutenção de registros completos e apropriados.

6.2.8 Na fase de registro e armazenamento, deverão ser realizadas as marcações e adotadas as demais medidas de salvaguarda das informações sigilosas nos termos da Lei 12.527/2011 ou de outras legislações específicas, bem como de informações pessoais.

6.2.9 As informações sigilosas classificadas, produzidas e armazenadas em meios eletrônicos, devem utilizar criptografia compatível com o grau de sigilo, conforme a legislação vigente.

6.2.10 No armazenamento de informações classificadas em grau de sigilo secreto ou ultrassecreto, deverá ser utilizado cofre ou estrutura que ofereça segurança equivalente.

6.2.11 No caso das demais informações sigilosas, o armazenamento deve ser realizado em ambiente com acesso controlado.

6.2.12 Os órgãos e entidades da APF devem instituir as medidas necessárias para garantir a segurança e o adequado tratamento das informações registradas e armazenadas em repositórios digitais institucionais, a fim de permitir o acesso, a recuperação e a preservação dessas informações.

6.2.13 As informações dos órgãos e entidades da APF devem ser armazenadas nos servidores de armazenamento e sistemas corporativos, instalados em ambiente seguro, que garantam a continuidade das atividades do órgão.

6.2.14 Em face de um cenário híbrido, que envolva ao mesmo tempo documentos em suporte físico e eletrônico, devem-se estabelecer requisitos de armazenamento que atendam às necessidades de preservação desses dois tipos de documentos.

6.2.15 Recomenda-se criteriosa e periódica avaliação na especificação de mídias de armazenamento adequadas à necessidade de preservação, atentando-se para a compatibilidade com as novas tecnologias.

6.2.16 Os órgãos e entidades da APF devem assegurar-se de que as informações hospedadas com uso de computação em nuvem estejam em conformidade com a legislação vigente.

6.3 Uso e disseminação

Os aspectos principais a serem observados pelos órgãos e entidades da APF na fase do uso e disseminação da informação são:

6.3.1 As informações deverão ser utilizadas para as finalidades para as quais foram produzidas e conforme os interesses dos órgãos e entidades da APF, não devendo ser usadas para propósito pessoal de determinado agente público ou privado.

6.3.2 Os órgãos e entidades da APF deverão garantir que as informações estejam disponíveis para a utilização pelos agentes públicos que delas necessitarem para o desempenho de suas atribuições.

6.3.3 Toda informação pública a ser disponibilizada por meio da transparência ativa deverá ser objeto de prévia avaliação a fim de que se identifiquem eventuais parcelas da informação que não sejam passíveis de divulgação.

6.3.4 O transporte e/ou a transferência de informações entre organizações deve respeitar os dispositivos previstos em atos normativos gerais que regulamentam o assunto, além de orientações específicas a cada órgão ou entidade da APF que se fizerem necessárias para que se garantam a preservação de informações de acesso restrito, a divulgação de informações ostensivas, e os princípios da disponibilidade, integridade, confidencialidade e autenticidade das informações.

6.3.5 A publicação de informações institucionais deve ser realizada prioritariamente por meio dos canais oficiais do órgão e entidade da APF.

6.3.6 Recomenda-se que os equipamentos de acesso franqueado ao público estejam em ambiente isolado da rede corporativa.

6.3.7 A concessão de acessos lógicos e físicos ou o uso de informações institucionais em dispositivos móveis corporativos e/ou particulares deve observar a legislação vigente.

6.3.8 Recomenda-se a regulamentação do uso de impressoras e copiadoras, definindo as diretrizes para a impressão/cópia de documentos que contenham informação de acesso restrito.

6.3.9 Recomenda-se a realização periódica de testes de restauração das informações contidas nas mídias de cópias de segurança, a fim de garantir seu uso quando da ocorrência de incidentes com comprometimento das informações.

6.3.10 No transporte de documentos em suporte físico que for realizado por empresas terceirizadas, cabe ao órgão e entidade da APF estabelecer contratualmente as medidas e procedimentos de SIC adequados.

6.3.11 Na definição dos procedimentos de segurança para o transporte de documentos, deve-se observar o tempo de exposição da informação, atentando-se para a agilidade, tempestividade e oportunidade.

6.3.12 Os órgãos e entidades da APF devem planejar e dimensionar seus sistemas e canais de comunicação de forma a garantir a disponibilidade das informações públicas distribuídas e/ou divulgadas.

6.3.13 Os órgãos e entidades da APF devem definir medidas e procedimentos para que os fluxos de distribuição das informações assegurem a continuidade das medidas de salvaguarda de informações sigilosas conforme a Lei 12.527/2011 ou de acordo com legislações específicas, bem como de informações pessoais relativas à intimidade, vida privada, honra e imagem detidas pelos órgãos e entidades da APF.

6.3.14 O acesso às áreas, instalações e materiais que contenham informações classificadas em qualquer grau de sigilo, ou que demandem proteção, nos termos da Seção VIII, do capítulo III do Decreto 7.845/2012 deve ser regulado e registrado.

6.3.15 No transporte de mídias que contenham informações sigilosas devem-se utilizar dispositivos com restrições de acesso e uso de criptografia adequada.

6.3.16 No transporte de documentos que contenham informações sigilosas, em qualquer suporte físico, os órgãos e entidades da APF deverão definir medidas e procedimentos de segurança adequados ao deslocamento.

6.4 Destinação

Os aspectos principais a serem observados pelos órgãos e entidades da APF na fase da destinação são:

6.4.1 As medidas referentes à destinação das informações produzidas ou custodiadas pelos órgãos e entidades da APF devem ser precedidas por avaliação que observe as orientações das legislações correlatas quanto ao encaminhamento necessário a cada tipo de registro, tais como documentos arquivísticos, materiais digitais, correios eletrônicos, entre outros, sob pena de responsabilização de agentes públicos que eliminarem registros de informações sem o devido fundamento legal.

6.4.2 Tal avaliação deve considerar aspectos como a temporalidade de guarda; os processos e as práticas a serem observados quando da guarda permanente; os procedimentos formais que precedem atos de eliminação; as orientações quanto à operacionalização do ato de eliminação, entre outros, devendo ser tais aspectos normatizados complementarmente pelos órgãos e entidades nos casos necessários e cabíveis.

6.4.3 A destinação de informações que constem de sítios eletrônicos institucionais, de repositórios internos da organização e/ou similares, deve observar as legislações correlatas sobre o assunto e, nos casos necessários, ser objeto de normatização complementar pelos órgãos e entidades da APF, para que se garanta a preservação de conteúdos relevantes para o exercício de suas competências e/ou a preservação de sua memória institucional.

6.4.4 Os órgãos e entidades da APF devem providenciar a sanitização de mídias, tais como dispositivos móveis, discos rígidos, memórias das impressoras, scanners, multifuncionais e demais dispositivos de armazenamento, antes de seu descarte, a fim de evitar a recuperação irregular de dados destes meios.

7 IMPLEMENTAÇÃO

A adoção de mecanismos de gestão dos processos e procedimentos envolvidos no tratamento da informação ao longo de seu ciclo de vida é fundamental para a implementação das diretrizes determinadas por esta norma. A metodologia aqui recomendada envolve os passos a seguir, a serem assegurados pela Alta Administração dos órgãos e entidades da APF:

7.1 Planejamento

7.1.1 A Alta Administração dos órgãos e entidades da APF deverá assegurar a elaboração de plano que defina as estratégias internas quanto ao tratamento da informação ao longo de seu ciclo de vida, visando à implementação das diretrizes determinadas por esta norma e dos dispositivos determinados por legislações correlatas ao tema.

7.1.2 O plano deverá identificar os objetivos e as ações necessárias ao aprimoramento do tratamento da informação durante o seu ciclo de vida no órgão ou entidade da APF, incluindo a indicação das ações de capacitação quanto ao tema, determinação de metas, indicadores e responsáveis, e a previsão de orçamento necessário à implementação do plano.

7.1.3 A elaboração do plano deverá envolver representantes, no mínimo, das áreas de gestão documental, segurança da informação, acesso a informação e controle interno.

7.1.4 O referido plano deve estar alinhado aos demais instrumentos de planejamento do órgão ou entidade da APF, como o Planejamento Estratégico, o Plano Diretor de Tecnologia da Informação e sua Política de Segurança da Informação e Comunicações, além de considerar o efeito das ações pretendidas sobre as fases do ciclo de vida da informação.

7.1.5 O plano deverá ser apreciado e aprovado pela Alta Administração dos órgãos e entidades da APF.

7.2 Execução

Aprovado o plano de ações conforme item anterior, deve-se garantir a sua implementação, incluindo a realização de ações de capacitação aos responsáveis pela sua execução, bem como dos demais agentes públicos quanto ao tratamento da informação no desempenho de suas atribuições.

7.3 Avaliação

7.3.1 Neste estágio, devem ser realizados procedimentos de avaliação da implementação das ações determinadas pelo plano, identificando-se as revisões e alterações pertinentes.

7.3.2 Após a realização da avaliação, devem ser elaborados os ajustes e as alterações cabíveis ao plano, a serem incorporadas após aprovação da Alta Administração do órgão ou entidade da APF.

7.3.3 Em seguida, devem ser implementadas as referidas alterações, assegurando-se de que atinjam os objetivos pretendidos.

8 VIGÊNCIA

Esta norma entra em vigor na data da sua publicação.

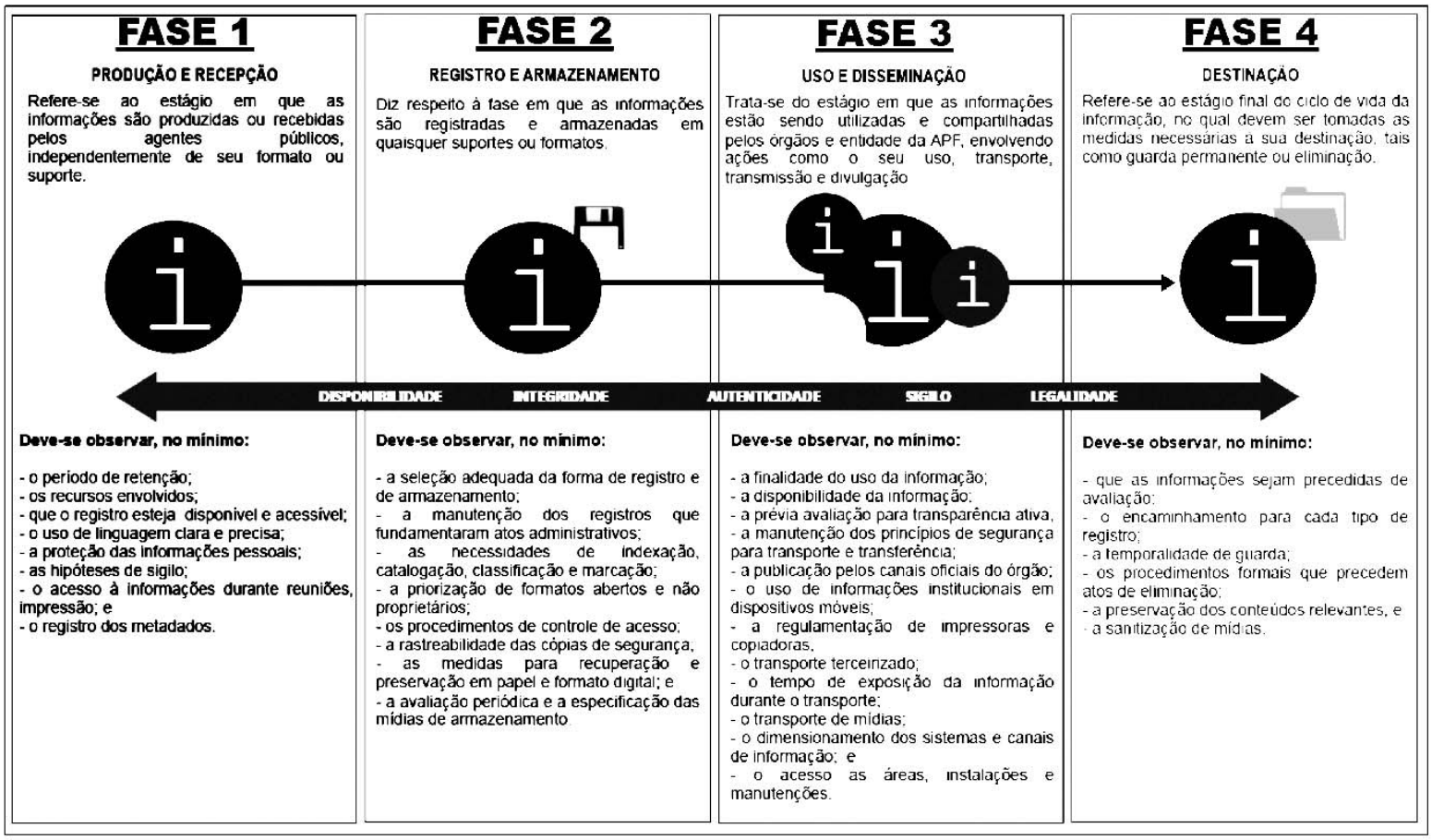
9 ANEXOS

A - Ciclo de Vida da Informação

B - Quadro Resumo e Embasamento Legal

ANEXO A

CICLO DE VIDA DA INFORMAÇÃO



ANEXO B

QUADRO RESUMO E EMBASAMENTO LEGAL

CLASSIFICADA	1.1 **Reservada -** Prazo máximo de restrição de acesso de 5 anos	Art. 23 e 24 da Lei 12.527/2011
	1.2 **Secreta -** Prazo máximo de restrição de acesso de 15 anos	Art. 23 e 24 da Lei 12.527/2011
	1.3 **Ultrassecreta -** Prazo máximo de restrição de acesso de 25 anos	Art. 23 e 24 da Lei 12.527/2011
ACESSO RESTRITO As hipóteses legais de restrição de acesso à informação elencadas neste item não são exaustivas	2.1 **Pessoal**	Art. 31 da Lei 12.527/2011
	2.2 **Protegida por Legislação Específica**	
	2.2.1 **Sigilos Decorrentes de Direitos de Personalidade**	
	2.2.1.1 Sigilo Fiscal	Art. 198 da Lei nº 5.172/1966
	2.2.1.2 Sigilo Bancário	Art. 1º da Lc nº 105/2001
	2.2.1.3 Sigilo Comercial	§2º do art. 155 da Lei nº 6.404/1976
	2.2.1.4 Sigilo Empresarial	Art. 169 da Lei nº 11.101/2005
	2.2.1.5 Sigilo Contábil	Art. 1.190 e 1.191 da Lei nº 5.869/1973
	2.2.2 **Sigilos de Processos e Procedimentos**	
	2.2.2.1 Restrição Discricionária de Acesso a Documento Preparatório	§ 3º do art. 7º da Lei nº 12.527/2011
	2.2.2.2 Sigilo do Procedimento Administrativo Disciplinar em Curso	Art. 150 da Lei nº 8.112/1991
	2.2.2.3 Sigilo do Inquérito Policial	Art. 20 da Lei nº 3.689/1941

	2.2.2.4 Segredo de Justiça no Processo Civil	Art. 155 da Lei nº 5.869/1973
	2.2.2.5 Segredo de Justiça no Processo Penal	§6º do art. 201 da Lei nº 3.689/1941
	2.2.3 **Informação de Natureza Patrimonial**	
	2.2.3.1 Segredo Industrial	Lei nº 9.279/1996
	2.2.3.2 Direito Autoral	Lei nº 9.610/1998
	2.2.3.3 Propriedade Intelectual - Software	Lei nº 9.609/1998
OSTENSIVA Todas as informações, com exceção das elencadas acima	3.1 **Transparência Ativa**	Art. 8º da Lei nº 12.527/2011
	3.2 **Transparência Passiva**	Art. 7º da Lei nº 12.527/2011