Tendo em vista o contido no Processo nº 00482.000099/2011-35; e

Considerando a jurisprudência iterativa do Superior Tribunal de Justiça e do Supremo Tribunal Federal, contrárias às teses já defendidas pelo Instituto Nacional do Seguro Social - INSS em juízo, edita a seguinte instrução, a ser observada pelos Procuradores Federais, na representação judicial do INSS:

Art. 1º Fica autorizada a desistência e a não interposição de recursos das decisões judiciais que, conferindo interpretação extensiva ao parágrafo único do art. 34 da Lei nº 10.741/2003, determinem a concessão do benefício previsto no art. 20 da Lei nº 8.742/93, nos seguintes casos:

I) quando requerido por idoso com 65 (sessenta e cinco) anos ou mais, não for considerado na aferição da renda *per capita* prevista no artigo 20, § 3º, da Lei n. 8.742/93:

a) o benefício assistencial, no valor de um salário mínimo, recebido por outro idoso com 65 anos ou mais, que faça parte do mesmo núcleo familiar;

b) o benefício assistencial, no valor de um salário mínimo, recebido por pessoa com deficiência, que faça parte do mesmo núcleo familiar;

c) o benefício previdenciário consistente em aposentadoria ou pensão por morte instituída por idoso, no valor de um salário mínimo, recebido por outro idoso com 65 anos ou mais, que faça parte do mesmo núcleo familiar;

II) quando requerido por pessoa com deficiência, não for considerado na aferição da renda *per capita* prevista no artigo 20, § 3º, da Lei n. 8.742/93 o benefício assistencial:

a) o benefício assistencial, no valor de um salário mínimo, recebido por idoso com 65 anos ou mais, que faça parte do mesmo núcleo familiar;

b) o benefício assistencial, no valor de um salário mínimo, recebido por pessoa com deficiência, que faça parte do mesmo núcleo familiar.

Art. 2º O disposto no artigo anterior não afasta a necessidade de discussão da matéria fática, devendo ser impugnada a decisão judicial fundamentada em acervo probatório que não comprove, de forma efetiva, a situação de miserabilidade do autor da ação.

Art. 3º Fica dispensada a propositura de ação rescisória contra as decisões judiciais transitadas em julgado nos termos do art. 1º desta Instrução Normativa.

PRESIDÊNCIA DA REPÚBLICA
CASA CIVIL
IMPRENSA NACIONAL

DILMA VANA ROUSSEFF
Presidenta da República

ALOIZIO MERCADANTE OLIVA
Ministro de Estado Chefe da Casa Civil

FERNANDO TOLENTINO DE SOUSA VIEIRA
Diretor-Geral da Imprensa Nacional

DIÁRIO OFICIAL DA UNIÃO

SEÇÃO 1
Publicação de atos normativos

SEÇÃO 2
Publicação de atos relativos a pessoal da Administração Pública Federal

SEÇÃO 3
Publicação de contratos, editais, avisos e ineditoriais

JORGE LUIZ ALENCAR GUERRA
Coordenador-Geral de Publicação e Divulgação

ALEXANDRE MIRANDA MACHADO
Coordenador de Editoração e Divulgação Eletrônica dos Jornais Oficiais

FRANCISCO DAS CHAGAS PINTO
Coordenador de Produção

A Imprensa Nacional não possui representantes autorizados para a comercialização de assinaturas impressas e eletrônicas

http://www.in.gov.br ouvidoria@in.gov.br
SIG, Quadra 6, Lote 800, CEP 70610-460, Brasília - DF
CNPJ: 04196645/0001-00
Fone: 0800 725 6787

Art. 4º Esta Instrução Normativa é de exclusiva observância por parte dos órgãos de contencioso da Procuradoria-Geral Federal, e não desobriga o oferecimento de resposta e a arguição de matérias processuais, prescrição, decadência, matérias do art. 301 do Código de Processo Civil e outras de ordem pública.

Art. 5º Esta Instrução Normativa entra em vigor na data de sua publicação no Diário Oficial da União.

LUIS INACIO LUCENA ADAMS

(*) Republicada por ter saído, no DOU nº 131, de 11/7/2014, Seção 1, pág 1, com incorreções no original.

PROCURADORIA-GERAL FEDERAL

PORTARIA Nº 507, DE 1º DE JULHO DE 2014

Altera a competência territorial da Procuradoria Federal no Estado do Ceará.

O PROCURADOR-GERAL FEDERAL, no uso da competência de que tratam os incisos I e VIII do § 2º do art. 11 da Lei nº 10.480, de 2 de julho de 2002, considerando o disposto na Portaria PGF nº 765, de 14 de agosto de 2008, e as alterações trazidas pela Portaria PGF nº 425, de 26 de maio de 2014, resolve:

Art. 1º A Procuradoria Federal no Estado do Ceará responderá, sem prejuízo de suas competências atuais, pelos municípios de Alto Santo, Aracati, Deputado Irapuan Pinheiro, Ererê, Fortim, Icapuí, Iracema, Itaiçaba, Jaguaretama, Jaguaribe, Jaguaruana, Jaguaribara, Limoeiro do Norte, Morada Nova, Palhano, Pereiro, Potiretama, Quixeré, Russas, São João do Jaguaribe, Solonópole, Tabuleiro do Norte.

Art. 2º A competência territorial atribuída à Procuradoria Federal no Estado do Ceará pelo art. 1º será realizada a partir da data de publicação desta Portaria até a conclusão da revisão da Portaria PGF nº 765, de 14 de agosto de 2008, alterada pela Portaria PGF nº 47, de 22 de janeiro de 2014.

Art. 3ª Esta Portaria entra em vigor na data de sua publicação, convalidando-se os atos anteriormente praticados.

MARCELO DE SIQUEIRA FREITAS

CONSELHO DE DEFESA NACIONAL
SECRETARIA EXECUTIVA

PORTARIA Nº 22, DE 15 DE JULHO DE 2014

Homologa a Revisão 01 da Norma Complementar nº 07/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 Revisão 01 da Norma Complementar nº 07/IN01/DSIC/GSIPR que estabelece diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações (SIC) 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 PARA IMPLEMENTAÇÃO DE CONTROLES DE ACESSO RELATIVOS À SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

ORIGEM
Departamento de Segurança da Informação e Comunicações

REFERÊNCIA LEGAL E NORMATIVA
Art. 6º da Lei nº 10.683, de 28 de maio de 2003;
Art. 6º do Anexo I do Decreto nº 8.100, de 4 de setembro de 2013;
Decreto nº 3.505, de 13 de junho de 2000;
Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008 e suas Normas Complementares;
NBR ISO/IEC 27001:2013 - Sistema de Gestão de Segurança da Informação;
NBR ISO/IEC 27002:2013 - Código de Práticas para a Gestão da Segurança da Informação.

CAMPO DE APLICAÇÃO
Esta Norma Complementar se aplica no âmbito da Administração Pública Federal, direta e indireta.

SUMÁRIO

INFORMAÇÕES ADICIONAIS
Anexo: Não há

APROVAÇÃO

RAPHAEL MANDARINO JUNIOR
Diretor do Departamento de Segurança da Informação e Comunicações

1. OBJETIVO

Estabelecer diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.

2. CONSIDERAÇÕES INICIAIS

2.1. O objetivo do controle é sistematizar a concessão de acesso, a fim de evitar a quebra de segurança da informação e comunicações.

2.2. A identificação, a autorização, a autenticação, o interesse do serviço e a necessidade de conhecer são condicionantes prévias para concessão de acesso nos órgãos ou entidades da APF.

2.3. A identificação dos controles de acesso lógico e físico, nos órgão ou entidade da APF, é consequência do processo de Gestão de Riscos de Segurança da Informação e Comunicações.

2.4. A implementação dos controles de acesso está condicionada à prévia aprovação pela autoridade responsável pelo órgão ou entidade da APF.

2.5. Para implementar os controles de acesso aprovados é fundamental a elaboração e divulgação de normas, bem como programas periódicos de sensibilização e conscientização em conformidade com a Política de Segurança da Informação e Comunicações dos órgãos ou entidades da APF.

2.6. Os órgãos ou entidades da APF, em suas áreas de competência, estabelecem regras específicas para credenciamento de acesso de usuários aos ativos de informação em conformidade com a legislação vigente, e em especial quanto ao acesso às informações em áreas e instalações consideradas críticas.

3. 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.

4. CONCEITOS E DEFINIÇÕES

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

4.1. 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.

4.2. Ativos de 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.

4.3. 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, dentre outros); algo que o usuário é (aferível por meios biométricos, tais como digitais, padrões de retina, reconhecimento facial, dentre outros).

4.4. Biometria: é a verificação da identidade de um indivíduo por meio de uma característica física ou comportamental única, através de métodos automatizados.

4.5. Bloqueio de acesso: processo que tem por finalidade suspender temporariamente o acesso.

4.6. Contas de Serviço: contas de acesso à rede corporativa de computadores necessárias a um procedimento automático (aplicação, script, etc.) sem qualquer intervenção humana no seu uso.

4.7. Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.

4.8. Credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer.

4.9. Credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha.

4.10. Exclusão de acesso: processo que tem por finalidade suspender definitivamente o acesso, incluindo o cancelamento do código de identificação e do perfil de acesso.

4.11. 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.

4.12. Necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação.

4.13. Perfil de acesso: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso.

4.14. Prestador de serviço: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso.

4.15. Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações.

4.16. Sistema de acesso: é um conjunto de ferramentas que se destina a controlar e dar permissão de acesso a uma pessoa a um local ou sistema.

4.17. Sistema biométrico: é um conjunto de ferramentas que se utiliza das características de uma pessoa, levando em consideração fatores comportamentais e fisiológicos, a fim de identificá-la de forma unívoca.

4.18. Termo de Responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso (Modelo - Anexo A).

4.19. Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

4.20. Usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade.

5. DIRETRIZES PARA IMPLEMENTAÇÃO DE CONTROLE DE ACESSO BIOMÉTRICO

5.1.1. A conta de acesso biométrico, quando implementada, deve ser vinculada a uma conta de acesso lógico e ambas devem ser utilizadas para se obter um acesso, a fim de atender os conceitos da autenticação de multifatores.

5.1.2. O órgão ou entidade deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

6. DIRETRIZES PARA CONTROLE DE ACESSO LÓGICO

6.1 Quanto à criação e administração de contas de acesso:

6.1.1. A criação de contas de acesso aos ativos de informação requer procedimentos prévios de credenciamento para qualquer usuário.

6.1.2. Disponibilizar ao usuário, que não exerce funções de administração da rede local, somente uma única conta institucional de acesso, pessoal e intransferível.

6.1.3. Utilizar conta de acesso no perfil de administrador somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

6.1.4. Responsabilizar o usuário pela quebra de segurança ocorrida com a utilização de sua respectiva conta de acesso, mediante assinatura de Termo de Responsabilidade (Modelo - Anexo A).

6.1.5. A criação de contas de serviço exige regras específicas vinculadas a um processo automatizado.

6.1.6. Os órgãos ou entidades da APF, em suas áreas de competência, estabelecem regras para credenciamento, bloqueio e exclusão de contas de acesso de seus usuários, bem como para o ambiente de desenvolvimento.

6.1.7. Recomenda-se a utilização de autenticação de multifatores para o controle de acesso lógico, a fim de autenticar a identidade de um usuário e vinculá-lo a uma conta de acesso a ativos de informação.

6.2. Quanto à rede corporativa de computadores:

6.2.1. Conceder credenciais de acesso à rede corporativa de computadores após a data de contratação ou de entrada em exercício do usuário.

6.2.2. Excluir credenciais de acesso à rede corporativa de computadores quando do desligamento do usuário.

6.2.3. Registrar os acessos à rede corporativa de computadores de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido em cada órgão ou entidade da APF.

6.2.4. Utilizar mecanismos automáticos para inibir que equipamentos externos se conectem na rede corporativa de computadores.

6.2.5. Manter, na rede corporativa, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados.

6.2.6. Utilizar a legislação específica para a concessão de acesso às informações sigilosas e para o acesso remoto, no âmbito da rede corporativa, por meio de canal seguro.

6.2.7. Gravar o acesso remoto à rede corporativa em logs para posterior auditoria, contendo informações específicas que facilitem o rastreamento da ação tomada;

6.2.8. Os órgãos ou entidades da APF, em suas áreas de competência, estabelecem regras para o uso de redes sem fio.

6.3. Quanto aos ativos de informação:

6.3.1. Conter ferramentas de proteção contra acesso não autorizado aos ativos de informação, que favoreça, preferencialmente, a administração de forma centralizada.

6.3.2. Respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação;

6.3.3. Utilizar ativo de informação homologado nas aplicações de controle de acesso, de tratamento das informações sigilosas e de criptografia;

6.3.4. Registrar eventos relevantes, previamente definidos, para a segurança e rastreamento de acesso às informações sigilosas.

6.3.5. Criar mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

6.3.6. O uso dos ativos de informação que não guarde relação com o exercício do cargo, função, emprego ou atividade públicas será considerado indevido e passível de imediato bloqueio de acesso, sem prejuízo da apuração das responsabilidades administrativa, penal e civil.

6.3.7. Os órgãos ou entidades da APF, em suas áreas de competência, estabelecem regras para o uso da Internet, do Correio Eletrônico e de Mensagens Instantâneas.

7. DIRETRIZES PARA CONTROLE DE ACESSO FÍSICO

7.1 Quanto às áreas e instalações físicas:

7.1.1. Os Órgãos ou entidades da APF estabelecem regras para o uso de credenciais físicas, que se destinam ao controle de acesso dos usuários às áreas e instalações sob suas responsabilidades;

7.1.2. Os Órgãos ou entidades da APF definem a necessidade e orientam a instalação de sistemas de detecção de intrusos nas áreas e instalações sob suas responsabilidades;

7.1.3. Classificar as áreas e instalações como ativos de informação de acordo com o valor, a criticidade, o tipo de ativo de informação e o grau de sigilo das informações que podem ser tratadas em tais áreas e instalações, mapeando aquelas áreas e instalações consideradas críticas;

7.1.4. Os Órgãos ou entidades da APF orientam o uso de barreiras físicas de segurança, bem como equipamentos ou mecanismos de controle de entrada e saída;

7.1.5. Proteger os ativos de informação contra ações de vandalismo, sabotagem, ataques, etc, especialmente em relação àqueles considerados críticos.

7.1.6. Implementar área de recepção com regras claras para a entrada e saída de pessoas, equipamentos e materiais;

7.1.7. Definir pontos de entrega e carregamento de material com acesso exclusivo ao pessoal credenciado;

7.1.8. Intensificar os controles para as áreas e instalações consideradas críticas em conformidade com a legislação vigente.

7.1.9. Para utilização de controle de acesso físico por meio de sistema biométrico são requeridos procedimentos prévios para o credenciamento do usuário. Esse recurso deve ser utilizado em conjunto com outro sistema de identificação (cartão, crachá, senha, chave, dentre outros), a fim de atender os conceitos da autenticação de multifatores.

7.2. Quanto aos usuários:

7.2.1. Difundir e exigir o cumprimento da Política de Segurança da Informação e Comunicações, das normas de segurança e da legislação vigente acerca do tema.

7.2.2. Conscientizar o usuário para adotar comportamento favorável à disponibilidade, à integridade, à confidencialidade e à autenticidade das informações.

7.2.3. Identificar e avaliar sistematicamente os riscos à segurança da informação e comunicações dos ativos de informação e quais controles devem ser aplicados quanto aos acessos dos usuários;

7.2.4. Estabelecer formulário específico de Termo de Responsabilidade (Modelo - Anexo A) a ser difundido e assinado individualmente pelos usuários;

7.2.5. Definir regras específicas para autorização de acesso e credenciamento dos usuários em conformidade com a classificação dos ativos de informação.

7.3. Quanto aos ativos de informação:

7.3.1. Estabelecer distância mínima de segurança para manutenção das mídias contendo as cópias de segurança (backups);

7.3.2. Classificar os ativos de informação em níveis de criticidade, considerando o tipo de ativo de informação, o provável impacto no caso de quebra de segurança, tomando como base a gestão de risco e a gestão de continuidade de negócios relativa aos aspectos da segurança da informação e comunicações da APF,

7.3.3. Um exemplo para classificação dos ativos de informação está disposto no Anexo B.

7.3.4. Os ativos de informação classificados como sigilosos requerem procedimentos especiais de controles de acesso físico em conformidade com a legislação vigente.

7.4. Quanto ao perímetro de segurança:

7.4.1. Definir perímetros de segurança, suas dimensões, equipamentos e tipos especiais de controles de acesso aos ativos de informação;

7.4.2. Ilustrar em documentação própria e permitir que sejam identificados os perímetros de segurança de cada ativo de informação por todos que transitarem ou tiverem acesso em tais espaços, em especial às áreas e instalações consideradas críticas;

7.4.3. Regulamentar, por intermédio de normas específicas de cada órgão ou entidade da APF, o armazenamento, a veiculação de imagem, vídeo ou áudio, registrados em perímetros de segurança.

8. VIGÊNCIA

Esta norma entra em vigor na data de sua publicação.

9. ANEXOS

A - Modelo de Termo de Responsabilidade

B - Modelo de Classificação de Ativos de Informação

ANEXO A - Modelo de Termo de Responsabilidade

SERVIÇO PÚBLICO FEDERAL
(Nome do órgão ou entidade da APF)

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em _____, e lotado no(a) _____ deste (Nome do órgão ou entidade), DECLARO , sob pena das sanções cabíveis nos termos da _____ (legislação vigente) que assumo a responsabilidade por:

I) tratar o(s) ativo(s) de informação como patrimônio do (Nome do órgão ou entidade);

II) utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do (Nome do órgão ou entidade);

III) contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;

IV) utilizar as credenciais, as contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do (Nome do órgão ou entidade);

V) responder, perante o (Nome do órgão ou entidade), pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

Local, UF, _____de _____de _____ .

_____
Assinatura
Nome do usuário e seu setor organizacional

_____
Assinatura
Nome da autoridade responsável pela autorização do acesso

ANEXO B - Modelo de Classificação de Ativos de Informação

Grau de criticidade	Ativos de informação	Impacto	Cor
Nível 1 - Alto	Data-center, servidores, central telefônica, recursos criptológicos, cópias de segurança, equipamentos de conectividade ou de armazenamento de informações ou de computação móvel das autoridades de primeiro escalão.	Interrompe a missão do órgão ou provoca grave dano à imagem institucional, à segurança do estado ou sociedade.	Vermelha
Nível 2 - Médio	Computadores com dados e informações únicas, de grande relevância, equipamentos de conectividade ou de armazenamento de informações ou de computação móvel das autoridades de segundo escalão.	Degrada o serviço do órgão ou provoca dano à imagem institucional, à segurança do estado ou sociedade.	Amarela
Nível 3 - Baixo	Os demais ativos de informação	Compromete planos ou provoca danos aos ativos de informação.	Sem cor

PORTARIA Nº 23, DE 15 DE JULHO DE 2014

Homologa a Revisão 02 da Norma Complementar nº 09/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 Revisão 02 da Norma Complementar nº 09/IN01/DSIC/GSIPR que estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações (SIC) 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

ORIENTAÇÕES ESPECÍFICAS PARA O USO DE RECURSOS CRIPTOGRÁFICOS EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

ORIGEM
Departamento de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA
Lei nº 12.527, de 18 de novembro de 2011
Decreto nº 3.505, de 13 de junho de 2000
Decreto nº 7.724, de 16 de maio de 2012
Decreto nº 7.845, de 14 de novembro de 2012
Instrução Normativa GSI nº 01 de 13 de junho de 2008 e suas respectivas Normas Complementares publicadas no DOU pelo DSIC/GSIPR.

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

Normatizar o uso de recurso criptográfico para a segurança de informações produzidas nos órgãos e entidades da Administração Pública Federal - APF, direta e indireta.

2. CONCEITOS E DEFINIÇÕES

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

2.1 Agente Responsável: servidor público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da APF, direta ou indireta, possuidor de credencial de segurança;

2.2 Algoritmo de Estado: função matemática utilizada na cifração e na decifração de informações sigilosas, necessariamente as informações classificadas, desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, não comercializável;

2.3 Algoritmo Registrado: função matemática utilizada na cifração e na decifração de informações não classificadas, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, cujo código fonte e método de processo sejam passíveis de controle e auditoria;

2.4 Chave Criptográfica: valor que trabalha com um algoritmo criptográfico para cifração ou decifração;

2.5 Cifração: ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem em claro, por outros ininteligíveis por pessoas não autorizadas a conhecê-la;

2.6 Credencial de Segurança: certificado que autoriza pessoa para o tratamento de informação classificada;

2.7 Decifração: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;

2.8 Empresa Estratégica de Defesa (EED) do setor de Tecnologia de Informação e Comunicação (TIC): toda pessoa jurídica do setor de Tecnologia de Informação e Comunicação (TIC) devidamente credenciada pelo Ministério da Defesa mediante o atendimento cumulativo das condições previstas no inciso IV do art. 2º da Lei nº 12.598, de 22 de março de 2012.

2.9 Gestor de Segurança da Informação e Comunicações: é responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF;

2.10 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, classificada como ultrassecreta, secreta ou reservada;

2.11 Informação Sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado; e

2.12 Recurso Criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração.

3. FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

Com fulcro no previsto pelo inciso II do art. 3º da Instrução Normativa nº 01, de 13 de junho de 2008, do Gabinete de Segurança Institucional da Presidência da República - GSI/PR, 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 APF, direta e indireta.

4. RESPONSABILIDADES

4.1 A Alta Administração dos órgãos e entidades da APF, direta e indireta, é responsável:

4.1.1 Pela utilização dos recursos criptográficos para a segurança das informações, principalmente as sigilosas, em conformidade com esta norma;

4.1.2 Por capacitar os Agentes Responsáveis para o uso dos recursos criptográficos, observando as normas vigentes, os procedimentos de credenciamento de segurança, e o tratamento de informação classificada; e,

4.1.3 Por prever recurso orçamentário para o uso de recursos criptográficos, conforme necessidade de cada órgão ou entidade.

4.2 O Gestor de Segurança da Informação e Comunicações dos órgãos e entidades da APF, direta e indireta, é responsável pela implementação dos procedimentos relativos ao uso de recursos criptográficos, em conformidade com as orientações contidas nesta norma e deve possuir credencial de segurança; e,

4.3 Todo Agente Responsável usuário de recurso criptográfico é encarregado pela sua operação e sigilo, deve possuir credencial de segurança e assinar o respectivo Termo de Uso de Recursos Criptográficos, conforme modelo constante no Anexo A.

5. ORIENTAÇÕES ESPECÍFICAS

Para fins de utilização de recursos criptográficos pelos órgãos e entidades da APF, direta e indireta, além da legislação aplicável, deverão ser observados os seguintes procedimentos:

5.1 Algoritmo de Estado:

5.1.1 Toda a informação classificada, em qualquer grau de sigilo, produzida, armazenada ou transmitida, em parte ou totalmente, por qualquer meio eletrônico, deverá obrigatoriamente ser protegida com recurso criptográfico baseado em algoritmo de Estado.

5.1.2 A cifração e decifração de informações classificadas, em qualquer grau de sigilo, utilizará exclusivamente recurso criptográfico baseado em algoritmo de Estado em conformidade com os parâmetros e padrões mínimos estabelecidos no Anexo B desta norma.

5.1.3 O transporte e a recepção de documento com informação classificada em grau de sigilo ultrassecreto serão efetuados pessoalmente por agente público autorizado, ou transmitidas por meio eletrônico, desde que sejam usados recursos de criptografia previsto no Anexo B, vedada sua postagem.

5.1.4 O canal de comunicação seguro (Rede Privada Virtual - VPN) que interligue redes dos órgãos e entidades da APF, direta e indireta, objetivando a troca de informações classificadas, deve utilizar recurso criptográfico baseado em algoritmo de Estado.

5.1.5 A utilização de recurso criptográfico, baseado em algoritmo de Estado, para cifração e decifração das informações não classificadas é opcional.

5.1.6 O Agente Responsável pela cifração ou decifração, no exercício do cargo, função, emprego ou atividade, utilizará recurso criptográfico baseado em algoritmo adotado pelo órgão ao qual está vinculado;

5.1.7 O uso de recurso criptográfico baseado em algoritmo de Estado é restrito ao Agente Responsável e requer treinamento e credenciamento de segurança, sob responsabilidade dos órgãos e entidades da APF, direta e indireta;

5.1.8 O credenciamento de estrangeiros para uso de recurso criptográfico baseado em algoritmo de Estado deve ser submetido ao GSI/PR;