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

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;

5.1.9 O GSI/PR é o órgão responsável pelo apoio técnico no tocante a atividades de caráter científico e tecnológico relacionadas ao recurso criptográfico baseado em algoritmo de Estado.

5.1.10 O recurso criptográfico, baseado em algoritmo de Estado, deverá ser de desenvolvimento próprio ou por órgãos e entidades da APF, direta ou indireta, mediante acordo ou termo de cooperação, vedada a participação e contratação de empresas e profissionais externos à APF, para tal finalidade.

5.1.11 Excepcionalmente, com anuência da Alta Administração do órgão ou entidade, o previsto no item 5.1.10 poderá ser terceirizado, desde que atendidas obrigatoriamente as seguintes condições:

a) seja uma Empresa Estratégica de Defesa do setor de Tecnologia de Informação e Comunicação e utilize tecnologia nacional, não sendo aceito empresas que apenas forneçam recursos criptográficos com tecnologia estrangeira;

b) seja realizado exclusivamente por meio de Contrato Sigiloso, nos termos dos arts. 48 e 49 do Decreto no 7.845, de 14 de novembro de 2012; e

c) seja previsto em cláusula contratual que fica vedado ao contratado os direitos de propriedade e de exploração comercial do recurso criptográfico com algoritmo de Estado objeto do referido contrato.

5.1.12 O não cumprimento do previsto no item 5.1.10 ou nas letras a, b e c do item 5.1.11, poderá gerar responsabilidade administrativa, civil e penal, conforme legislação vigente.

5.1.13 A Alta Administração dos órgãos e entidades da APF deverá prever explicitamente nos entendimentos, contratos, termos ou acordos de aquisição e manutenção de equipamentos, dispositivos móveis, sistemas, aplicativos ou serviços que disporão de recurso criptográfico baseado em algoritmo de Estado, o fiel cumprimento do disposto na presente norma, sem prejuízo da legislação vigente.

5.1.14 Além do disposto nesta norma, os recursos criptográficos baseados em algoritmo de Estado podem ser objeto de regulamentação específica.

5.2 Algoritmo Registrado:

5.2.1 A cifração e decifração das informações sigilosas não classificadas deve utilizar recurso criptográfico, no mínimo, baseado em algoritmo registrado, desde que atendidas obrigatoriamente as seguintes condições:

a) O desenvolvimento ou obtenção do algoritmo registrado deverá ser realizado levando-se em consideração a necessidade de proteção da informação sigilosa, bem como as possíveis ameaças à sua exposição, cabendo tal responsabilidade a alta administração do órgão que o empregará; e

b) O algoritmo deverá ser registrado no GSI/PR, que manterá sob sua guarda e controle o banco de registros;

c) O órgão deverá manter sob sua guarda o código fonte e método de processos do algoritmo, bem como implementar os controles adequados, inclusive quanto à auditoria;

5.3 Toda informação sigilosa – classificada ou não –, independente do algoritmo de criptografia utilizado, somente poderá ser armazenada em centro de processamento de dados fornecido por órgãos e entidades da Administração Pública Federal, conforme legislação em vigor.

5.4 É vedado ao Agente Responsável por recurso criptográfico nos órgãos e entidades da APF, direta e indireta:

5.4.1 utilizar recursos criptográficos em desacordo com esta norma, bem como, com a legislação em vigor; e

5.4.2 utilizar recursos criptográficos diferentes dos parâmetros e padrões mínimos definidos pelo órgão ou entidade da APF, direta e indireta, a que pertence.

6. CONTROLE

6.1 Todo recurso criptográfico constitui material de acesso restrito e requer procedimentos especiais de controle para o seu acesso, manutenção, armazenamento, transferência, trânsito e descarte, em conformidade com a legislação vigente.

6.2 A Alta Administração dos órgãos e entidades da APF deverá:

6.2.1 enviar para o GSI/PR relatório de conformidade relativo à aderência a presente norma de todos os recursos criptográficos baseados em algoritmo de Estado sob sua responsabilidade, ao serem adquiridos, quando solicitado e com periodicidade estabelecida por aquele Gabinete;

6.2.2 enviar para o GSI/PR relatório relativo aos procedimentos aplicados no tratamento de informação classificada previstos no art. 41 do Decreto 7.845, de 14 de novembro de 2012, quando solicitado e com periodicidade estabelecida por aquele Gabinete ou, oportunamente, por iniciativa do próprio órgão, quando ocorrer o previsto nos incisos IV e V do mesmo artigo;

6.2.3 informar ao GSI/PR, tempestivamente, o comprometimento do sigilo de qualquer recurso criptográfico baseado em algoritmo de Estado;

7. DISPOSITIVOS TRANSITÓRIOS:

7.1 A Alta Administração dos órgãos e entidades da APF, direta e indireta, providenciará a adequação dos recursos criptográficos já em uso, no prazo máximo de 180 dias, contados a partir da publicação do guia técnico de recursos criptográficos previsto no item 7.3;

7.2 Os órgãos e entidades deverão adotar os recursos criptográficos baseados em algoritmo de Estado com parâmetros e padrões de que trata o Anexo B no prazo de um ano a contar da publicação da presente norma;

7.3 O GSI/PR coordenará a elaboração, em 90 (noventa) dias, prorrogáveis por igual período, de um guia técnico de recursos criptográficos como orientações de como proceder para cumprir o previsto no item 5.2.

8. VIGÊNCIA

Esta norma entra em vigor na data de sua publicação.

9. ANEXOS

A - Modelo de Termo de Uso de Recurso Criptográfico

B - Padrões mínimos para recurso criptográfico baseado em algoritmo de Estado

ANEXO A

Modelo de Termo de Uso de Recurso Criptográfico

SERVIÇO PÚBLICO FEDERAL

(Nome do órgão ou entidade da APF)

TERMO DE USO DE RECURSO CRIPTOGRÁFICO

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 e nos termos da _____ (legislação vigente) que TENHO conhecimento sobre o uso do recurso criptográfico sob minha responsabilidade, sendo vedado seu uso:

I) para fins diversos dos funcionais ou institucionais;

II) para interceptar ou tentar interceptar transmissão de dados ou informações não destinados ao seu próprio acesso por quaisquer meios;

III) para tentar ou efetuar a interferência em serviços de outros usuários ou o seu bloqueio por quaisquer meios;

IV) para violar ou tentar violar os recursos de segurança dos equipamentos que utilizem recursos criptográficos;

V) para cifração ou decifração de informações ilícitas, entre os quais, materiais obscenos, ofensivos, ilegais, não éticos, ameaças, difamação, injúria, racismo ou quaisquer que venham a causar molestamento, tormento ou danos a terceiros;

VI) de forma inadequada, expondo-o a choques elétricos ou magnéticos, líquidos ou outros fatores que possam vir a causar-lhes danos, incluindo testes de invasão/intrusão/penetração, teste de quebra de senhas, teste de quebra de cifração, e teste de técnicas de invasão e defesa entre outros;

Local, UF, _____de _____de _____ .

Assinatura

_____

Nome do usuário e seu setor organizacional

ANEXO B

Padrões mínimos para recurso criptográfico baseado em algoritmo de Estado

TABELA I - Tamanho da chave:

Nível de segurança da Informação	RSA/LD	Curvas Elípticas
Reservado	2048	224
Secreto	3248	256
Ultrassecreto	Não recomendado	Não recomendado

TABELA II - Algoritmos de bloco:

Classificação	Algoritmo	
	Chave	Bloco
Reservado	192	128
Secreto	256	128
Ultrassecreto	Não recomendado	

TABELA III - Algoritmos sequenciais:

Classificação	Algoritmo
Reservado	192
Secreto	256
Ultrassecreto	Não recomendado

TABELA IV – Sistema de Chave Única:

Classificação	Algoritmo
Ultrassecreto	Sequência aleatória