Instrução Normativa GSI/PR nº 3, de 06 de março de 2013.

Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.

O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA - GSI/PR, no uso de suas atribuições;

Considerando:

- o disposto nos incisos II do art. 37 da Lei nº 12.527, de 18 de novembro de 2011;
- o disposto no Decreto nº 3.505, de 13 de junho de 2000;
- o disposto no inciso II do *caput* do art. 70 do Decreto nº 7.724, de 16 de maio de 2012;
- o disposto no art. 40 e seu parágrafo único e no art. 56 do Decreto nº 7.845, de 14 de novembro de 2012;
- o disposto na Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008;
- o disposto na Norma Complementar - NC 09/IN01/DSIC/GSI/PR (Revisão 01), de 15 fevereiro de 2013; e
- a necessidade de orientar a condução de políticas de segurança da informação classificada, já existentes, ou a serem implementadas pelos órgãos e entidades do Poder Executivo Federal;

RESOLVE:

Art. 1º Estabelecer, no âmbito do Poder Executivo Federal, os parâmetros e padrões mínimos para recursos criptográficos baseados em algoritmos de Estado, que deverão ser implementados, pelos órgãos e entidades, na criptografia da informação classificada, em qualquer grau de sigilo.

Art. 2º Para fins desta Instrução Normativa - IN entende-se por:

I - **Agente Responsável**: servidor público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade do Poder Executivo Federal e possuidor de credencial de segurança;

II - **Algoritmo de Estado**: função matemática utilizada na cifração e na decifração, desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades do Poder Executivo Federal;

III - **Chave Criptográfica**: valor que trabalha com um algoritmo criptográfico para cifração ou decifração;

IV - **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;

V - **Credencial de Segurança**: certificado que autoriza pessoa para o tratamento da informação classificada;

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

VII - **Gestor de Segurança da Informação e Comunicações**: é o responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade do Poder Executivo Federal;

VIII - **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; e

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

Art. 3º A Alta Administração dos órgãos e entidades do Poder Executivo Federal, sob pena de responsabilidade, deverá, no âmbito de sua competência, assegurar a implementação e utilização dos parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado, para criptografia da informação classificada, em qualquer grau de sigilo;

Parágrafo único. O Gestor de Segurança da Informação e Comunicações e todo Agente Responsável, usuários de recurso criptográfico baseado em algoritmo de Estado, devem seguir o disposto nesta Instrução Normativa e na legislação vigente, sob pena de responsabilidade.

Art. 4º A cifração e decifração de informações classificadas, em qualquer grau de sigilo, devem utilizar recurso criptográfico baseado em algoritmo de Estado em conformidade com os padrões e parâmetros mínimos estabelecidos na NC 09/IN01/DSIC/GSI/PR (Revisão 01), de fevereiro de 2013, reproduzidos no Anexo desta Instrução Normativa.

Art. 5º O recurso criptográfico baseado em algoritmo de Estado deverá ser de desenvolvimento próprio ou por órgãos e entidades do Poder Executivo Federal, mediante acordo ou termo de cooperação, vedada a participação e contratação de empresas e profissionais externos, para tal finalidade.

§ 1º Excepcionalmente, com anuência da Alta Administração do órgão ou entidade, o previsto no *caput* poderá ser terceirizado, desde que atendidas obrigatoriamente as seguintes condições:

I - 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;

II - 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 presente contrato;

§ 2º O não cumprimento do previsto no *caput* ou nos incisos I e II do § 1°, poderá gerar responsabilidade administrativa, civil e penal, conforme legislação vigente.

Art. 6º À Alta Administração dos órgãos e entidades do Poder Executivo Federal compete:

I - solicitar, quando se fizer necessário, apoio técnico ao GSI/PR, referente ao uso de recurso criptográfico baseado em algoritmo de Estado, para o cumprimento da legislação pertinente;

II - realizar autoavaliação de conformidade relativa ao uso dos recursos criptográficos baseados em algoritmo de Estado, e encaminhar relatório anual ao GSI/PR, conforme previsto no item 5.6.2 da NC 09/IN01/DSIC/GSI/PR (Revisão 01), de fevereiro de 2013;

III - adequar os recursos criptográficos, já em uso, às determinações desta Instrução Normativa, e conforme legislação vigente;

IV - 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 Instrução Normativa, sem prejuízo da legislação vigente;

V - garantir o previsto no art. 41 do Decreto nº 7.845, de 14 de novembro de 2012, e encaminhar relatório anual ao GSI/PR, conforme previsto no item 5.6.3 da NC 09/IN01/DSIC/GSI/PR (Revisão 01), de fevereiro de 2013;

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

VII - 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

VIII - prever recurso orçamentário para o uso de recursos criptográficos baseados em algoritmos de Estado, conforme necessidade de cada órgão ou entidade.

Art. 7º O GSI/PR acompanhará periodicamente o cumprimento do estabelecido nesta IN pelos órgãos e entidades do Poder Executivo Federal, por meio do disposto no item 5.6 da NC 09/IN01/DSIC/GSI/PR (Revisão 01), de 15 de fevereiro de 2013, e de visitas técnicas quando se fizer necessário.

Art. 8º O GSI/PR prestará apoio técnico, previsto no art. 56 do Decreto nº 7.845, de 14 de novembro de 2012, devendo os órgãos e entidades do Poder Executivo Federal formalizarem a demanda junto ao GSI/PR no prazo de até cento e oitenta dias, conforme previsto no item 5.9.3 da NC 09/IN01/DSIC/GSI/PR (Revisão 01), de 15 de fevereiro de 2013.

Parágrafo único. Vencido o prazo do *caput*, as necessidades recebidas não serão mais tratadas como demanda específica para o cumprimento do prazo referido no Decreto, e sim, como demanda de caráter ordinário.

Art. 9º Todo recurso criptográfico baseado em algoritmo de Estado constitui material de acesso restrito e requer procedimentos especiais adequados de controle para o seu acesso, manutenção, armazenamento, transferência, trânsito e descarte, em conformidade com a legislação vigente, sob pena de responsabilização da Alta Administração.

Parágrafo único. O Gestor de Segurança da Informação e Comunicações e todo Agente Responsável, usuários de recurso criptográfico baseado em algoritmo de Estado, devem possuir credencial de segurança, ou excepcionalmente, assinar o Termo de Compromisso de Manutenção de Sigilo - TCMS, conforme Anexo I do Decreto nº 7.845, de 14 de novembro de 2012.

Art. 10 Esta Instrução Normativa entra em vigor na data de sua publicação.

JOSÉ ELITO CARVALHO SIQUEIRA

ANEXO

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