GSI/PR Normative Instruction nº 3, of March 6, 2013.

Provides for the minimum parameters and standards of cryptographic resources based on State algorithms for encryption of information classified within the scope of the Federal Executive Branch.

THE MINISTER OF STATE HEAD OF THE INSTITUTIONAL SECURITY CABINET OF THE PRESIDENCY OF THE REPUBLIC - GSI/PR, in the use of its powers;

Considering:

• the provisions of items II of art. 37 of Law nº 12,527 , of November 18, 2011;
• the provisions of Decree nº 3,505, of June 13, 2000;
• the provisions of item II of the caput of art. 70 of Decree nº 7,724, of May 16, 2012;
• the provisions of art. 40 and its sole paragraph and in art. 56 of Decree nº 7,845, of 14 November 2012;
• the provisions of Normative Instruction GSI/PR nº 1, of June 13, 2008;
• the provisions of the Complementary Standard - NC 09/IN01/DSIC/GSI/PR (Revision 01), of February 15, 2013; and
• the need to guide the conduct of classified information security policies, already existing, or to be implemented by bodies and entities of the Federal Executive Branch;

RESOLVES:

Art. 1 Establish, within the scope of the Federal Executive Branch, the minimum parameters and standards for cryptographic resources based on State algorithms, which must be implemented, by bodies and entities, in the encryption of classified information, to any degree of secrecy.

Art. 2 For the purposes of this Normative Instruction - IN is understood as:
I - **Responsible Agent**: public servant occupying a permanent or military career position in a body or entity of the Federal Executive Branch and holding a security clearance;
II - **State Algorithm**: mathematical function used in encryption and decipherment, developed
by the State, for exclusive use in the interest of the service of bodies or entities of the Federal Executive Branch;
III - **Cryptographic Key**: value that works with a cryptographic algorithm for encryption or decryption;
IV - **Encryption**: act of encrypting through the use of a symmetric or asymmetric algorithm, with cryptographic resources, to replace clear language signs with others that are unintelligible by people not authorized to know it;
V - **Security Clearance**: certificate that authorizes a person to process the classified information;
VI - **Decryption**: act of deciphering using a symmetric or asymmetric algorithm, with cryptographic resources, to reverse the original encryption process;

VII - **Information and Communications Security Manager**: is responsible for information and communications security actions within the scope of the body or entity of the Federal Executive Branch;
VIII - **Classified Information**: confidential information held by public bodies and entities, observing its content and due to its essentiality to the security of society or the State, classified as Ultrassecreto, Secreto or Reservado; and
IX - **Cryptographic Resource**: system, program, process, equipment isolated or in network that uses a symmetric or asymmetric algorithm to perform encryption or decryption.

Art. 3 The Senior Administration of the bodies and entities of the Federal Executive Branch, under penalty of liability, must, within the scope of its competence, ensure the implementation and use of the minimum parameters and standards of cryptographic resources based on State algorithms, for encryption of the classified information, to any degree of secrecy;
Sole paragraph. The Information and Communications Security Manager and every Responsible Agent, users of a cryptographic resource based on a State algorithm, must follow the provisions of this Normative Instruction and current legislation, under penalty of liability.

Art. 4 The encryption and decryption of classified information, at any level of secrecy, must use cryptographic resources based on a State algorithm in accordance with the standards and minimum parameters established in NC 09/IN01/DSIC/GSI/PR (Revision 01), February 2013, reproduced in the Annex to this Normative Instruction.

Art. 5 The cryptographic resource based on a State algorithm must be developed in-house or by bodies and entities of the Federal Executive Branch, through an agreement or cooperation term, with the participation and hiring of external companies and professionals prohibited for this purpose.
§ 1 Exceptionally, with the approval of the Senior Management of the body or entity, the provisions of the caput may be outsourced, provided that the following conditions are complied with:
I - is carried out exclusively through a Confidential Contract, in accordance with arts. 48 and 49 of Decree nº 7,845 , of November 14, 2012;
II - it is provided for in a contractual clause that the contractor is prohibited from the rights of ownership and commercial exploitation of the cryptographic resource with state algorithm, object of this contract;
§ 2 Failure to comply with the provisions of the caput or in items I and II of § 1 may result in administrative, civil and criminal liability, in accordance with current legislation.

Art. 6 The Senior Management of the bodies and entities of the Federal Executive Power is responsible for:
I - request, when necessary, technical support from the GSI/PR, regarding the use of a cryptographic resource based on a State algorithm, to comply with the relevant legislation;
II - carry out a self-assessment of compliance regarding the use of cryptographic resources based on a State algorithm, and forward an annual report to the GSI/PR, as provided for in item 5.6.2 of NC 09/ IN01/DSIC/GSI/PR (Revision 01), February 2013;

III - adapt the cryptographic resources, already in use, to the determinations of this Instruction Normative, and in accordance with current legislation;
IV - explicitly provide in the understandings, contracts, terms or agreements for the acquisition and maintenance of equipment, mobile devices, systems, applications or services that will have a cryptographic resource based on a State algorithm, the faithful compliance with the provisions of this Normative Instruction, without prejudice current legislation;
V - guarantee the provisions of art. 41 of Decree nº 7,845, of November 14, 2012, and forward the annual report to the GSI/PR, as provided for in item 5.6.3 of NC 09/IN01/DSIC/GSI/PR (Revision 01), of February 2013;
VI - inform the GSI/PR, in a timely manner, of the compromised secrecy of any cryptographic resource based on a State algorithm;
VII - train Responsible Agents to use cryptographic resources, observing current standards, security accreditation procedures, and the treatment of classified information; and
VIII - provide budgetary resources for the use of cryptographic resources based on State algorithms, according to the needs of each body or entity.

Art. 7 The GSI/PR will periodically monitor compliance with the provisions of this IN by the bodies and entities of the Federal Executive Branch, through the provisions of item 5.6 of NC 09/IN01/DSIC/ GSI/PR (Revision 01), of 15 February 2013, and technical visits when necessary.

Art. 8 The GSI/PR will provide technical support, provided for in art. 56 of Decree nº 7,845, of November 14, 2012, and the bodies and entities of the Federal Executive Branch must formalize the demand with the GSI/PR within a period of up to one hundred and eighty days, as provided for in item 5.9.3 of NC 09/ IN01/DSIC/GSI/PR (Revision 01), of February 15, 2013.
Sole paragraph. Once the deadline in the caput has expired, the needs received will no longer be treated as a specific demand to comply with the deadline referred to in the Decree, but rather as an ordinary demand.

Art. 9 Every cryptographic resource based on a State algorithm constitutes material with restricted access and requires appropriate special control procedures for its access, maintenance, storage, transfer, transit and disposal, in accordance with current legislation, under penalty of liability of the High administration.
Sole paragraph. The Information and Communications Security Manager and every Responsible Agent, users of a cryptographic resource based on a State algorithm, must have a security credential, or exceptionally, sign the Secrecy Maintenance Commitment Term - TCMS, as per Annex I of Decree nº. 7,845, of November 14, 2012.

Art. 10 This Normative Instruction comes into force on the date of its publication.

JOSÉ ELITO CARVALHO SIQUEIRA

ANNEX

Minimum Standards for Stateful Algorithm-Based Cryptographic Resource

TABLE I - Key size:

Security Level of Information	RSA/LD	Ellipticals Curves
Reservado	2048	224
Secreto	3248	256
Ultrassecreto	No recommended	No recommended

TABLE II - Block algorithms:

Classification	Algorithm	
	Key	Block
Reservado	192	128
Secreto	256	128
Ultrassecreto	No recommended	

TABLE III - Sequential algorithms:

Classification	Algorithm
Reservado	192
Secreto	256
Ultrassecreto	No recommended

TABLE IV - Single Key System:

Classification	Algorithm
Ultrassecreto	Random sequence