MINISTERIO DE INDUSTRIA Y COMERCIO

GOBIERNO NACIONAL
Construyendo el futuro hoy

NORMAS DE ALGORITMOS CRIPTOGRÁFICOS PKI-PARAGUAY

(DOC PKI-06)

Versión 1.0

CONTROL DOCUMENTAL

Documento	
Título: Normas de algoritmos Criptográficos PKI-Paraguay	**Nombre del archivo:**
Código: DOC PKI-06	**Soporte Lógico:**
Fecha: 28/10/2016	**Ubicación Física**: DGFD y CE
Versión: 1.0	

Registro de Cambios		
Versión	**Fecha**	**Motivo de Cambio**

Distribución del documento	
Nombre	**Área**
Ministerio de Industria y Comercio (MIC)	Dirección General de Firma Digital y Comercio Electrónico (DGFD y CE)
Autoridad Certificadora (CA)	Prestadores de Servicio de Certificación (PSC)
Documento Público	www.acraiz.gov.py

Control del Documento		
Preparado por:	**Revisado por:**	**Aceptado por:**
Ing. Lucas Sotomayor	***M.Sc. Mario Monges***	***M. Sc. Rodys Rolón***

Contenido

Acrónimo	Descripción
CA	Autoridad de Certificación (CA por sus siglas en inglés, Certificate Authority)
CA Raíz	Autoridad Certificadora Raíz del Paraguay
CAdES	CMS Advanced Eletronic Signature
CBC	Cipher Block Chaining
CP	Política de Certificación (CP por sus siglas en inglés, Certificate Policy)
CPS	Declaración de Prácticas de Certificación (CPS por sus siglas en inglés, Certification Practice Statement)
DOC-PKI	Documentos principales de la Infraestructura de Claves Publicas del Paraguay
DGFDyCE	Dirección General de Firma Digital y Comercio Electrónico dependiente del Vice Ministerio de Comercio.
GCM	Galois/Conter Mode
MIC	Ministerio de Industria y Comercio
PAdES	PDF Advanced Eletronic Signature
PIN	Número de Identificación Personal, (por sus siglas en inglés, Personal Identification Number).
PKI Paraguay	Infraestructura de Claves Públicas del Paraguay (PKI por sus siglas en inglés, Public Key Infrastructure).
PSC	Prestador de Servicios de Certificación.
RSA	Rivest, Shamir and Adleman Algorithm
SHA	Secure Hash Algorithm
XAdES	XML Advanced Eletronic Signature

1. INTRODUCCIÓN

Este documento regula el estándar de hardware, algoritmos y parámetros criptográficos que serán utilizados en todos los procesos realizados en el ámbito de la Infraestructura de Claves Públicas del Paraguay (PKI Paragua), que incluyen, entre otros:

a) generación de claves criptográficas;
b) solicitud, emisión y revocación de certificados digitales;
c) generación y verificación de firmas digitales;
d) cifrado de mensajes;
e) autenticación con certificados digitales.

Las directrices contenidas en este documento deben ser cumplidas obligatoriamente por las autoridades de certificación (CA), autoridades de registro (RA), prestadores de servicios de soporte (PSS), las empresas de Auditoría Independiente y otros organismos acreditados o registrados ante la PKI Paraguay a través del Ministerio de Industria y comercio, así como también por los titulares finales y los desarrolladores de aplicaciones que utilizan certificados digitales de PKI Paraguay.

2. APLICABILIDAD DE LOS ALGORITMOS Y PARAMETROS CRIPTOGRÁFICOS

Esta sección relaciona los principales procedimientos que involucra a la criptografía en el ámbito de la PKI Paraguay, con los algoritmos y parámetros que deben ser utilizados obligatoriamente**,** para su ejecución, y los documentos normativos que tratan dichos procedimientos.

Solicitud de certificados a la CA	
Normativa PKI Paraguay	DOC-PKI-02- ítem 4.1.1 CP CA Raíz
	DOC-PKI-02- ítem 6.1.3 CP CA Raíz
	DOC-PKI-04- ítem 6.1.3 directiva CP
Formato	Estándar PKCS#10

Entrega de certificados emitidos por la CA	
Normativa PKI Paraguay	DOC-PKI-02- item 4.3.1
	DOC-PKI-02- item 6.1.4
	DOC-PKI-03- ítem 6.1.4 directiva CPS
	DOC-PKI-04- ítem 6.1.4
Formato	Estándar PKCS#7

Generación de las Claves Asimétricas de la CA	
Normativa PKI Paraguay	DOC-PKI-02- item 6.1.1
	DOC-PKI-02- item 6.1.5
	DOC-PKI-04- ítem 6.1.1
Algoritmo	RSA conforme al RFC 5639
Tamaño de clave	RSA 4096

Generación de las Claves Asimétricas de Usuarios finales	
Normativa PKI Paraguay	DOC-PKI-04- ítem 6.1.5
Algoritmo	RSA conforme al RFC 5639
Tamaño de clave F1 y C1	RSA 2048
Tamaño de clave F2 y C2	RSA 2048, RSA 4096

Firma de certificados de la CA	
Normativa PKI Paraguay	DOC-PKI-02- ítem 7.1.3
	DOC-PKI-03- ítem 7.1.3
Suite de Firmas	sha256WithRSAEncryption sha512WithRSAEncryption

Firma de certificados de Usuarios Finales	
Normativa PKI Paraguay	DOC-PKI-04- ítem 7.1.3
Suite de Firmas	sha256WithRSAEncryption sha512WithRSAEncryption

Firma de Listas de Certificados Revocados y Respuestas OCSP	
Normativa PKI Paraguay	DOC-PKI-02- ítem 7.2
	DOC-PKI-03- ítem 7.2
	DOC-PKI-04- ítem 7.2
Suite de Firmas	sha256WithRSAEncryption sha512WithRSAEncryption

Guarda de la clave privada de la entidad titular y de su Backup	
Normativa PKI Paraguay	DOC-PKI-04- ítem 6.1.1
	DOC-PKI-04- ítem 6.2.4
	DOC-PKI-03- ítem 6.2.4
Algoritmo y tamaño de clave	3DES – 112 bits AES – 128 o 256 bits
Modo de operación	CBC o GCM

Firma Digital de la PKI Paraguay CAdES, XAdES y PAdES	
Función de Resumen (Función HASH)	SHA - 1 SHA - 256 SHA - 512
Suite de Firmas	sha1WithRSAEncryption sha256WithRSAEncryption sha512WithRSAEncryption

Esquema de acuerdo de claves
RSA 2048
RSA 4096

Esquema de envelopes Criptográficos
3desWithRSA1024Encryption
3desWithRSA2048Encryption
aes128WithRSA2048Encryption
aes256WithRSA4096Encryption

3. ESTANDARES DE HARDWARE

En la siguiente tabla se relaciona los estándares mínimos a ser empleados en los hardwares criptográficos utilizados en la PKI Paraguay con los documentos normativos que tratan su uso.

Utilización	Requisito obligatorio	Estándares	Norma
Módulo criptográfico de generación de claves asimétricas para usuario final	Homologado por el MIC	FIPS 140-1 o FIPS 140-2 (para certificados tipo F1 o C1). FIPS 140-2 nivel 2 o nivel 3 (para certificados tipo F2 o C2).	DOC-PKI-03 item 6.2.1 DOC-PKI-04 Ítem 6.2.1
Módulo criptográfico para almacenamiento de la clave privada del titular del certificado	Homologado por el MIC	FIPS 140-1 o FIPS 140-2 (para certificados tipo F1 o C1). FIPS 140-2 nivel 2 o nivel 3 (para certificados tipo F2 o C2).	DOC-PKI-04 ítem 6.8
Parámetro de generación de claves asimétricas de usuario final	Homologado por el MIC	FIPS 140-1 o FIPS 140-2 (para certificados tipo F1 o C1). FIPS 140-2 nivel 2 o nivel 3 (para certificados tipo F2 o C2).	DOC- PKI -04 ítem 6.1.6
Módulo criptográfico de generación de claves asimétricas para el PSC	Homologado por el MIC	FIPS 140-2 nivel 3	DOC-PKI-03 ítem 6.2.1
Módulo criptográfico para almacenamiento de la clave privada del PSC	Homologado por el MIC	FIPS 140-2 nivel 3	DOC-PKI-03 ítem 6.8

Parámetro de generación de claves asimétricas del PSC	Homologado por el MIC	FIPS 140-2 nivel 3	DOC- PKI -03 ítem 6.1.6
Módulo criptográfico de generación de claves asimétricas para CA raíz.		FIPS 140-2 nivel 3	DOC- PKI-02 ítem 6.2.1
Módulo criptográfico para almacenamiento de la clave privada de la CA raíz.		FIPS 140-2 nivel 3	DOC- PKI-02 ítem 6.8
Parámetro de generación de claves asimétricas de la CA raíz.		FIPS 140-2 nivel 3	DOC- PKI-02 ítem 6.1.6
Proceso para Verificación de parámetros de generación de claves asimétricas de la CA raíz		FIPS 140-2 nivel 3	DOC- PKI-02 item 6.1.6 DOC- PKI-03 item 6.1.6 DOC- PKI-04 item 6.1.6