NORMAS DE ALGORITMOS CRIPTOGRÁFICOS DE LA ICPP

DOC-ICPP-06

Versión 1.0

Firmado digitalmente por PEDRO BENJAMIN MANCUELLO PEREZ

CONTROL DOCUMENTAL

Documento	
Título: Normas de algoritmos Criptográficos ICPP	**Nombre Archivo:** DOC-ICPP-06 V1.0
Código: DOC-ICPP-06	**Soporte Lógico:** https://www.acraiz.gov.py/
Fecha: 04/08/2022	**Versión:** 1.0

Registro de Cambios		
Versión	**Fecha**	**Motivo de Cambio**
1.0	04/08/2022	Versión inicial

Distribución del documento	
Nombre	**Área**
Ministerio de Industria y Comercio (MIC)	Dirección General de Comercio Electrónico (DGCE)
Autoridad Certificadora (AC)	Prestadores cualificados de Servicios de Confianza (PCSC)
Documento Público	https://www.acraiz.gov.py/

Control del documento	
Elaborado por: ***JENNY RUÍZ DÍAZ***	Firmado digitalmente por JENNY ELIZABETH RUIZ DIAZ LEZCANO Fecha: 2022.08.04 16:00:42 -04'00'
Verificado por: ***LUJAN OJEDA***	MARIA LUJAN OJEDA CHAMORRO Digitally signed by MARIA LUJAN OJEDA CHAMORRO Date: 2022.08.04 15:31:51 -04'00'
Aprobado por: ***LUCAS SOTOMAYOR***	LUCAS ATILIO SOTOMAYOR LLANO Firmado digitalmente por LUCAS ATILIO SOTOMAYOR LLANO Fecha: 2022.08.04 17:10:23 -03'00'

Contenido

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 (ICPP), 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; y
e) autenticación con certificados digitales.

Las directrices contenidas en este documento deben ser cumplidas obligatoriamente por las autoridades de certificación (AC Raíz-Py y PCSC), autoridades de registro (ARs), prestadores de servicios de soporte (PSSs), el Organismo de Evaluación de la Conformidad (OEC) y otros organismos acreditados o registrados ante la ICPP a través del Ministerio de Industria y Comercio, así como también por los titulares o responsables de certificados electrónicos emitidos en el marco de la ICPP y los desarrolladores de aplicaciones que utilizan certificados digitales de ICPP.

2. SIGLAS Y ACRÓNIMOS

Sigla/Acrónimo	Descripción
AC	Autoridad de Certificación (CA por sus siglas en inglés, Certificate Authority)
AC Raíz-Py	Autoridad Certificadora Raíz del Paraguay
AR	Autoridad de Registro
CAdES	CMS Advanced Electronic Signature
CBC	Cipher Block Chaining
CP	Política de Certificación (CP por sus siglas en inglés, Certificate Policy)
DOC-ICPP	Documentos principales de la Infraestructura de Claves Públicas del Paraguay
DGCE	Dirección General de Comercio Electrónico dependiente del Viceministerio de Comercio y Servicios.
GCM	Galois/Conter Mode

MIC	Ministerio de Industria y Comercio
OCSP	Protocolo de estado de certificado en línea (On-line Certificate Status Protocol)
PAdES	(PDF Firma Electrónica Avanzada) PDF Advanced Electronic Signature
PKCS	Estándares de criptografía de clave pública (Public Key Cryptgraphy Standards)
ICP	Infraestructura de Claves Públicas (PKI por sus siglas en inglés, Public Key Infrastructure).
ICPP	Infraestructura de Claves Públicas del Paraguay
PCSC	Prestador Cualificado de Servicios de Confianza
PSS	Prestador de Servicios de Soporte
RFC	Solicitud de comentarios (Request For Comments)
RSA	Rivest, Shamir and Adleman Algorithm
SHA	Algoritmo hash seguro (Secure Hash Algorithm)
XAdES	Firma Electrónica Avanzada XML (XML Advanced Electronic Signature)

3. APLICABILIDAD DE LOS ALGORITMOS Y PARÁMETROS CRIPTOGRÁFICOS

Esta sección relaciona los principales procedimientos que involucran a la criptografía en el ámbito de la ICPP, 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 AC	
Normativa ICPP	DOC-ICPP-01 [1] - ítem 4.1.1
	DOC-ICPP-01 [1] - ítem 6.1.3
	DOC-ICPP-03 [2] - ítem 6.1.3
	DOC-ICPP-04 [3] - ítem 6.1.3
Formato	Estándar PKCS#10

Entrega de certificados emitidos por la AC

Normativa ICPP	DOC-ICPP-01 [1] - ítem 4.3.1
	DOC-ICPP-01 [1] - ítem 6.1.4
	DOC-PKI-03 [2] - ítem 6.1.4
	DOC-PKI-04 [3] - ítem 6.1.4
Formato	Estándar PKCS#7

Generación de las Claves Asimétricas de la AC	
Normativa ICPP	DOC-ICPP-01 [1] - ítem 6.1.1
	DOC-ICPP-01 [1] - ítem 6.1.5
	DOC-ICPP-03 [2] - ítem 6.1.5
	DOC-ICPP-04 [3] - ítem 6.1.5
Algoritmo	RSA
Tamaño de clave	RSA 4096

Generación de las Claves Asimétricas de Usuarios finales

Normativa ICPP	DOC-ICPP-04 [3] - ítem 6.1.5
	DOC-ICPP-04 [3] - ítem 6.1.1
	DOC-ICPP-08 [5] - ítem 7.5
Algoritmo	RSA
Tamaño de clave F1	RSA 2048
Tamaño de clave F2, F3, S2 y S3	RSA 2048 o RSA 4096

Firma o Sellado de Certificados de la AC	
Normativa ICPP	DOC-ICPP-01 [1] - ítem 7.1.3
	DOC-ICPP-03 [2] - ítem 7.1.3
Suite de Firmas	sha256WithRSAEncryption sha512WithRSAEncryption

Firma o Sello de certificados de Usuarios Finales	
Normativa ICPP	DOC-ICPP-04 [3] - ítem 7.1.3
Suite de Firmas	sha256WithRSAEncryption

	sha512WithRSAEncryption

Firma o Sello de Listas de Certificados Revocados LCR y Respuestas OCSP	
Normativa ICPP	DOC-ICPP-01 [1] - ítem 7.2 y 7.3
	DOC-ICPP-03 [2] - ítem 7.2 y 7.3
	DOC-ICPP-04 [3] - ítem 7.2 y 7.3
Suite de Firmas	sha256WithRSAEncryption sha512WithRSAEncryption

Guarda de la Clave Privada de la entidad titular y de su Backup	
Normativa ICPP	DOC-ICPP-04 [3] - ítem 6.1.1
	DOC-ICPP-04 [3] - ítem 6.2.4
	DOC-ICPP-03 [2] - ítem 6.2.4
Algoritmo y tamaño de clave	3DES – 112 bits AES – 128 o 256 bits
Modo de operación	CBC o GCM

Firma o Sello en el marco de la ICPP CAdES, XAdES y PAdES	
Normativa ICPP	DOC-ICPP-08 [5] - ítem 7.6
Tipo de certificado	F1, F2 y F3, S2,S3
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

4. ESTÁNDARES DE HARDWARE

En la siguiente tabla se relacionan los estándares mínimos a ser empleados en los hardware criptográficos utilizados en la ICPP con los documentos normativos que tratan su uso.

Utilización	Requisito obligatorio	Estándares	Norma
Módulo criptográfico de generación de claves asimétricas de usuario final titular del certificado.	Certificado por el MIC	● FIPS 140-1 o FIPS 140-2 (para certificados tipo F1). ● FIPS 140-2 nivel 2 o nivel 3 (para certificados tipo F2 y S2). ● FIPS 140-2 nivel 3 (para certificados	DOC-ICPP-03 [2] - ítem 6.2.1 DOC-ICPP-04 [3] - Ítem 6.2.1 DOC-ICPP-07 [4] - Ítem 6.4 DOC-ICPP-08 [5] - Ítem 7.3

		tipo (F2,F3, S2 o S3).	
Módulo criptográfico para almacenamiento de la clave privada del usuario final titular del certificado.	Certificado por el MIC	• FIPS 140-2 nivel 2 o nivel 1 (para certificados tipo F1). • FIPS 140-2 nivel 2 o nivel 3 (para certificados tipo F2 o S2). • FIPS 140-2 nivel 3 (para certificados tipo F2,F3, S2 o S3).	DOC-ICPP-04 [3] - ítem 6.2.1 y 6.2.7 DOC-ICPP-07 [4] - Ítem 6.4 DOC-ICPP-08 [5] - Ítem 7.3
Parámetro de generación de claves asimétricas de usuario final titular del certificado.	Certificado por el MIC	• FIPS 140-1 o FIPS 140-2 (para certificados tipo F1). • FIPS 140-2 nivel 2 o nivel 3 (para certificados tipo F2 o S2). • FIPS 140-2 nivel 3 (para certificados tipo F2,F3, S2 o S3).	DOC- ICPP-04 [3] - ítem 6.1.6 DOC-ICPP-07 [4] - Ítem 6.4 DOC-ICPP-08 [5] - Ítem 7.3
Módulo criptográfico de	Certificado por el MIC		DOC-ICPP-03 [2] - ítem 6.2.1

generación de claves asimétricas para el PCSC.		● FIPS 140-2 nivel 3	
Módulo criptográfico para almacenamiento de la clave privada del PCSC.	Certificado por el MIC	● FIPS 140-2 nivel 3	DOC-ICPP-03 [2] - ítem 6.2.7
Parámetro de generación de claves asimétricas del PSC	Certificado por el MIC	● FIPS 140-2 nivel 3	DOC- ICPP-03 [2] - ítem 6.1.6
Módulo criptográfico de generación de claves asimétricas para AC Raíz-Py.		● FIPS 140-2 nivel 3	DOC- ICPP-01 [1] - ítem 6.2.1
Módulo criptográfico para almacenamiento de la clave privada de la AC Raíz-Py.		● FIPS 140-2 nivel 3	DOC- ICPP-01 [1] - ítem 6.8
Parámetro de generación de		● FIPS 140-2 nivel 3	DOC- ICPP-01 [1] - ítem 6.1.6

claves asimétricas de la AC Raíz-Py.			
Proceso para Verificación de parámetros de generación de claves asimétricas de la AC Raíz-Py.		● FIPS 140-2 nivel 3	DOC- ICPP-01 [1] - ítem 6.1.6 DOC- ICPP-03 [2] - ítem 6.1.6 DOC- ICPP-04 [3] - ítem 6.1.6

5. DOCUMENTOS DE REFERENCIA

5.1. REFERENCIAS

- Ley N° 6822/2021 "De los servicios de confianza para las transacciones electrónicas, del documento electrónico y los documentos transmisibles electrónicos".

5.2. REFERENCIAS A DOCUMENTOS QUE COMPONEN LA PKI-Paraguay

Tabla - Documentos Referenciados

REF.	NOMBRE DEL DOCUMENTO	CÓDIGO
[1]	Declaración de Prácticas de certificación de la AC Raíz de la ICPP.	DOC-ICPP-01

[2]	Directivas obligatorias para la formulación y elaboración de la declaración de prácticas de certificación de los prestadores de servicios de certificación de la ICPP.	DOC-ICPP-03
[3]	Directivas obligatorias para la formulación y elaboración de la política de certificación de los prestadores de servicios de certificación de la ICPP.	DOC-ICPP-04
[4]	Procedimientos operacionales mínimos para el servicio de generación o gestión de datos de creación de firma electrónica y/o sello electrónico	DOC-ICPP-08
[5]	Directivas obligatorias para la formulación y elaboración de la declaración de prácticas de certificación del PCSC que genera o gestiona datos de creación de firma electrónica y/o de sello electrónico	DOC-ICPP-07