ANEXO X
ESTÁNDARES RECONOCIDOS PARA LA ACREDITACIÓN

Los estándares criptográficos recomendados se listan en el estándar ETSI TS 102 176 -1, a excepción de los algoritmos de generación de claves RSA 1024, HASH MD5 y SHA-1[1].

[1] Recomendación publicada por el National Institute of Standards and Technology

Estándar	**Propósito**
EC/PKI	
RFC 3280, RFC 3279	Certificados de firma
RFC 5280, RFC 3279, RFC 4325, RFC 4630, RFC 4055, RFC 4491, RFC 5480, RFC 5758	Lista de Certificados Revocados
RFC 2560	Respuesta OCSP
RFC 3280, RFC 3279	Certificados de Entidad de Certificación
RFC 3161, TS 101 861	Peticiones de Sellos de tiempo
RFC 3161, TS 101 861, RFC 5816	Certificados de Unidades de Sellado de tiempo
RFC 3280, RFC 3279	Certificados auto-firmados para certificados de TSU (unidades de sellado de tiempo)
RFC 3280, RFC 3279	Certificado de atributos
RFC 3281	Certificado de autoridad de atributos
sha 224 sha 384 sha 512 sha 256	Algoritmos de resumen, para la identificación de documentos firmados.
RSA 2048, RSA 4096, DSA, ECDSA	Generación de claves asimétricas.
ETSI TS 102 778	Formato de firma electrónica avanzada en PDF - PAdES

(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf)

ETSI TS 101 733	Formato de firma electrónica avanzada - CAdES
ETSI TS 101 903	Formato de firma electrónica avanzada en XML - XAdES
DSA, FIPS 186-4	Algoritmo de firma digital
RSA, FIPS 186-3	Algoritmo de firma digital RSA
ECDSA, FIPS 186-3	Algoritmo de firma digital de Curvas Elípticas
ETSI TS 102 918	Associated Signature Containers
EN 419211-2-2014	Perfiles de protección para dispositivos de creación de firma segura – Parte 2: Dispositivos con generación de clave
EN 419211-3-2014	Perfiles de protección para dispositivos de creación de firma segura – Parte 3: Dispositivos con importación de clave
EN 419211-4-2014	Perfiles de protección para dispositivos de creación de firma segura – Parte 4: Extensión para dispositivos con generación de claves y canal seguro para la aplicación de creación de firma
ETSI TS 102 176-1	Algoritmos y parámetros para firmas electrónicas seguras Parte 1: Funciones de Hash y algoritmos asimétricos
ETSI TS 102 023	Requerimientos de política para autoridades de sellado de tiempo
ETSI TS 101 861	Perfil del sello de tiempo
ETSI TR 102 038	Formato XML para políticas de firma
ETSI TR 102 041	Reporte de políticas de firma
ETSI TR 102 045	Política de firma para modelo de negocio extendido
ETSI TR 102 272	Formato ASN.1 para políticas de firma
IETF RFC 2560, X.509	Protocolo de Estado de Certificado en Línea - OCSP

IETF RFC 3125	Políticas de firma electrónica
RFC 5652, RFC 4853, RFC 3852	Sintaxis del mensaje criptográfico (CMS)
ITU-T Recommendation X.680	Abstract Syntax Notation ONE (ASN.1).
ETSI TS 101862, IETF RFC 3739, RFC 3279, RFC 5756	Perfil de certificados cualificados
ETSI TS 102280 x.509 v.3	Perfil de certificados emitidos para personas naturales
IETF RFC 4055	Algoritmos e identificadores adicionales para Criptografía RSA para el uso en la Internet X.509 Certificado de Infraestructura de la Clave pública y Perfil de Lista de Certificados Revocados (CRL)
SP 800-102	Recomendación para las líneas de tiempo de la firma digital
RFC 3647	Sistema básico de Política de Certificados y Prácticas de Certificación X.509 para PKI
PKCS#1	Estándar criptográfico RSA
PKCS#3	Estándar Diffie-Hellman para el acuerdo de claves
PKCS#6	Estándar de sintaxis de extensiones de certificado
PKCS#7	Estándar de sintaxis de mensaje criptográfico
PKCS#8	Estándar de sintaxis de información de clave privada
PKCS#9	Tipo de atributos seleccionados
PKCS#10	Estándar de petición de certificado
PKCS#11	Interface de token criptográfico

PKCS#12	Estándar de sintaxis de intercambio de información personal
PKCS#13	Estándar de criptografía de curvas elípticas
PKCS#15	Estándar de formato de información de token criptográfico
TSL	
ETSI TS 102 231	Proveedor de información sobre confianza de servicios
ETSI TS 101 456	Políticas para AC que expiden certificados reconocidos
ETSI TR 102 040	Armonización internacional de políticas para las AC que expiden certificados
Tarjetas Inteligentes	
EN 14890-2:2009, ISO/IEC 15946 series, ISO/IEC 7816-4:2005, 7816-8:2004, 7816-9:2004	Interface para tarjetas inteligentes como dispositivos de creación segura de firma digital
Ceritificaciones	
ISO 20000	Gestión de tecnología
Webtrust	Certificación de evaluación de Entidades de Certificación
CMMI	Estándar que define procesos de calidad en el ciclo de vida de desarrollo de software
Common Criteria EAL	Seguridad de las aplicaciones de software
ISO 27001	Sistemas de gestión de seguridad de la información
ISO 21188	Infraestructura de llave pública para servicios financieros - Estructura de prácticas y políticas

ISO 27002	Tecnología de la información - Código de prácticas para la gestión de la seguridad de la información
ISO 9000	Estándar que define procesos de calidad
HSM	
FIPS 140-2	Seguridad de módulos criptográficos
Aplicaciones Web	
OWASP Top Ten, OWASP Testing Project	Seguridad de Aplicaciones Web

(*) A efectos de los procedimientos de acreditación y seguimiento; debe tomarse en cuenta que las últimas versiones de los estándares utilizados serán los vigentes.