ENTIDAD DE CERTIFICACIÓN DEL CONSEJO DE LA JUDICATURA ICERT-EC

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN SELLADO DE TIEMPO

ICERT - EC ENTIDAD DE CERTIFICACIÓN Consejo de la Judicatura	***DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN SELLADO DE TIEMPO***	*Versión: 3.0*
		Fecha: 08-09-2016
		OID: 1.3.6.1.4.1.43745.2.1

Código	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-14-A.05-DEC2.1-2Declaración de Prácticas de Certificación Sellado de Tiempo	Declaración de Prácticas de Certificación Sellado de Tiempo Versión 2.0	Octubre 2014	septiembre 2016

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
2014-06-02	1.0	**CONSEJO DE LA JUDICATURA** David Moncayo	
2014-10-17	2.0	**CONSEJO DE LA JUDICATURA** David Moncayo Flor Chancay	Se realizó actualización de la documentación presentada ante SENATEL para obtener la acreditación.
2014-09-08	3.0	**CONSEJO DE LA JUDICATURA** David Moncayo Flor Chancay	Se realizó actualización según Acuerdo MINTEL No. 012-2016 de 23 de mayo de 2016 .

Firmas de responsabilidad

	Nombre	Cargo	Firma
Creado por:	David Moncayo	Jefe Unidad	
Creado por:	Flor Chancay	Analista 2	
Revisado por:	Reynaldo Gaibor	Subdirector Nacional de Seguridad de la Información	
Aprobado por:	Tomás Alvear	Director General	

Código	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-14-A.05-DEC2.1-2Declaración de Prácticas de Certificación Sellado de Tiempo	Declaración de Prácticas de Certificación Sellado de Tiempo Versión 2.0	Octubre 2014	septiembre 2016

Contenido

Código	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-14-A.05-DEC2.1-2Declaración de Prácticas de Certificación Sellado de Tiempo	Declaración de Prácticas de Certificación Sellado de Tiempo Versión 2.0	Octubre 2014	septiembre 2016

Código	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-14-A.05-DEC2.1-2Declaración de Prácticas de Certificación Sellado de Tiempo	Declaración de Prácticas de Certificación Sellado de Tiempo Versión 2.0	Octubre 2014	septiembre 2016

1. Introducción

1.1. Objeto

El presente documento reúne las disposiciones establecidas por la Autoridad de Sellado de Tiempo de la ICERT-EC para la emisión de tokens que contienen sellos de tiempo firmados. Se establece en el documento su ámbito de aplicación y los participantes de este proceso especificando sus responsabilidades y derechos.

La presente política se ha desarrollado de conformidad a lo establecido en la RFC-3628 "*Requeriments for time-stamping authorities*".

Esta política está basada en certificados emitidos bajo la norma X.509 v3.

1.2. Nombre del documento e identificación

Este documento se denomina Declaración de Prácticas de Certificación – Sellado de Tiempo, el cual contiene la siguiente información que podrá ser consultada en la página web de la ICERT- EC www.icert.fje.gob.ec.

NOMBRE DEL DOCUMENTO	*DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN SELLADO DE TIEMPO*
Identificador OID	*1.3.6.1.4.1.43745.2.1*
Versión	*3.0*
Fecha de emisión	*09 septiembre de 2016*
Ubicación URL	http://www.icert.fje.gob.ec/dpc/declaracion_practicas_sellado_tiempo.pdf

1.3. Entidad que administra el certificado

La Subdirección Nacional de Seguridad de la Información es la instancia que administra la presente Declaración de Prácticas de Certificación – Sellado de Tiempo, encargada también de la elaboración, registro, mantenimiento y actualización del documento.

Los datos de la Entidad para información al respecto son:

ENTIDAD DE CERTIFICACIÓN	*ENTIDAD DE CERTIFICACION ICERT - EC*
NOMBRE	*Subdirección Nacional de Seguridad de la Información*
DIRECCIÓN	*Av. 12 de Octubre N24-563 y Francisco Salazar*
TELÉFONO	*+593 2 395 3600*
E-mail	entidad.certificacion@funcionjudicial.gob.ec

Código	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-14-A.05-DEC2.1-2Declaración de Prácticas de Certificación Sellado de Tiempo	Declaración de Prácticas de Certificación Sellado de Tiempo Versión 2.0	Octubre 2014	septiembre 2016

1.4. Persona de contacto

Los datos de la persona de contacto disponible para suministrar información son:

ENTIDAD DE CERTIFICACIÓN	*ENTIDAD DE CERTIFICACION ICERT - EC*
NOMBRE	*Ing. Reynaldo Gaibor* *Sudirector Nacional de Seguridad de la Información*
DIRECCIÓN	*Av. 12 de Octubre N24-563 y Francisco Salazar*
TELÉFONO	*+593 2 395 3600*
E-mail	entidad.certificacion@funcionjudicial.gob.ec

Código	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-14-A.05-DEC2.1-2Declaración de Prácticas de Certificación Sellado de Tiempo	Declaración de Prácticas de Certificación Sellado de Tiempo Versión 2.0	Octubre 2014	septiembre 2016

2. Referencias

La presente Declaración de Prácticas de Certificación Sellado de Tiempo (DPC-ST) está fundamentada en las normas y en las recomendaciones contenidas en los siguientes documentos:

[DPC]	Declaración de Prácticas de Certificación de la ICERT-EC
[X.509]	Norma de la UIT que regula la interconexión de los sistemas de procesamiento de información con el fin de proporcionar servicios de directorio. Para su aplicación en Infraestructura de Clave Pública la norma desarrolla el marco al que deben regirse las Declaraciones de Prácticas de Certificación y las Políticas de Certificado.
[RFC2560]	RFC 2560. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. June 1999.
[RFC3161]	RFC 3161. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). August 2001.
[RFC3628]	RFC 3628. Internet X.509 Public Key Infrastructure Time-Stamp Authorities (TSAs). August 2001.
[RFC3629]	RFC 3629. UTF-8, a transformation format of ISO 10646. November 2003.
[RFC5280]	RFC 5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. May 2008.
[CWA14167-1]	CWA 14167-1. Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements. June 2003.
[LEY2002-67]	Ley No. 2002-67. Ley de comercio electrónico, firmas electrónicas y mensajes de datos
[DECRETO3496]	Decreto No. 3496. Reglamento a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos.
[DECRETO1356]	Decreto Nº 1356. Reformas al Reglamento general a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos.
[DECRETO867]	Decreto Nº 867. Reforma al Reglamento general a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos. Registro Oficial Nº 532.
[MINTEL181]	Ministerio de Telecomunicaciones y de la Sociedad de la Información. Acuerdo Nº 181.
[MINTEL12]	Ministerio de Telecomunicaciones y de la Sociedad de la Información. Acuerdo Nº 12 de 23 de mayo de 2016.
[P-CERT]	Firma Electrónica CJ Ecuador - Perfiles de certificado y CRL - versión 2.0. 17/10/2014.

Código	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-14-A.05-DEC2.1-2Declaración de Prácticas de Certificación Sellado de Tiempo	Declaración de Prácticas de Certificación Sellado de Tiempo Versión 2.0	Octubre 2014	septiembre 2016

3. Definiciones y siglas

3.1. Definiciones

En el desarrollo de la presente DPC los términos empleados son los siguientes:

Autoridad de Certificación (AC): Entidad encargada de emitir y revocar certificados digitales utilizados en firma electrónica y cuya clave pública está incluida en el.

Autoridad de Registro (AR): Entidad encarga de receptar las solicitudes de certificados, identificar y autenticar la información de los solicitantes de certificados, aprobar o rechazar las solicitudes de certificados, revocar o suspender certificados o en determinadas circunstancias, y aprobar o rechazar las solicitudes para renovar o volver a introducir su certificados.

Autoridad de Sellado de Tiempo: Sistema de emisión y gestión de sellos de tiempo seguros.

Cadena de confianza: También conocida como Jerarquía de Confianza la constituyen las autoridades de certificación relacionadas por la confiabilidad en la emisión de certificados digitales entre diferentes niveles jerárquicos. En el caso del CJ existen la Autoridad de Certificación Raíz y la Autoridad de Certificación Subordinada.

Clave privada: En un criptosistema de claves públicas es la clave, de un par de claves de un usuario, que es conocida solamente por el usuario o titular del certificado.

Clave pública: En un criptosistema de claves públicas es la clave, de un par de claves de un usuario, que se conoce públicamente y aparece en un directorio público. La clave pública pertenece a la CA, se incluye en el certificado digital.

CRL (Certificate Revocation List): Lista de certificados que han sido revocados.

Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de la Ley 67.

Datos personales autorizados: Son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, hecho que debe constar expresamente señalado y ser aceptado por dicho titular.

Declaración de Prácticas de Sellado de Tiempo: Declaración de las prácticas que una Autoridad de Sellado de Tiempo emplea en la emisión de sus sellos.

HSM (Hardware Security Module): Es el componente o dispositivo criptográfico utilizado para generar, almacenar y proteger claves criptográficas.

OCSP (Online Certificate Status Protocol): Protocolo informático utilizado para comprobar el estado de un certificado digital en el momento en que es utilizado. Proporciona información actualizada y complementaria del estatus de certificados revocados.

OID (Object Identifier): El Identificador de Objetos constituye el valor de una secuencia de componentes variables utilizado para nombrar a casi cualquier tipo de objeto en los certificados digitales, tales como los componentes de los nombres distinguidos, DPC, etc.

PKCS (Public Key Cryptography Standard): Estándares de criptografía de claves públicas.

PKCS #10: Estándar de criptografía de clave pública utilizado para procesar la petición de un certificado y solicitar la generación de una clave.

PKCS #12: Estándar de criptografía de clave pública que define un formato de fichero utilizado para almacenar claves privadas con su certificado de clave pública protegido mediante clave simétrica.

PKI (Public Key Infrastructure): La Infraestructura de Clave Pública es el conjunto de elementos informáticos (hardware y software), políticas y procedimientos necesarios para brindar servicios de certificación digital.

Política de certificados: Documento que complementa la Declaración de Prácticas de Certificación y que contiene un conjunto de reglas que norman las condiciones de uso y los procedimientos seguidos por la ICERT-EC para la emisión de certificados, determinando la aplicabilidad de un certificado a una grupo o comunidad en particular y/o a una clase de aplicaciones con requisitos comunes de seguridad.

RFC (Request for comments): Publicaciones de *Internet Engineering Task Force* que en forma de memorandos contienen protocolos y procedimientos para regular el funcionamiento de Internet.

Sellado de tiempo: Anotación firmada electrónicamente y agregada a un mensaje de datos mediante procedimientos criptográficos en la que consta como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación, basándose en el RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

Suscriptor: Persona o entidad que solicita los servicios proporcionados por la Autoridad de Sellado de Tiempo dela ICERT-EC.

Time-Stamping Service: Un servicio que genera y provee tokens de sellado de tiempo.

Token de sello de tiempo: Dispositivo empleado en un proceso de creación de firma electrónica que vincula la representación de un dato a un tiempo concreto, estableciendo de esta manera la existencia de ese dato antes de ese tiempo.

Usuario: Destinatario de un token de sello de tiempo que confía en el mismo.

X.509: Estándar desarrollado por la UIT-T para infraestructuras de claves públicas que especifica entre otros temas, los formatos estándar para certificados de claves públicas y para la implementación de listas de certificados revocados.

3.2. Siglas

AC: Autoridad de Certificación

AD (Active Directory): Directorio Activo

AR: Autoridad de Registro

AV: Autoridad de Validación

BD: Base de datos

C (Country) País: Atributo del DN de un objeto dentro de la estructura de directorio X.500.

CAdES: CMS Advanced Electronic Signature

CAdES-X: CAdES with eXtended validation data

CAdES-XL: CAdES-X Long

CN (Common Name) Nombre Común: Atributo del DN de un objeto dentro de la estructura de directorio X.500.

CRL (Certificate Revocation List): Lista de Certificados Revocados

DN (Distinguished Name) Nombre distintivo: Identificación unívoca de una entrada dentro de un directorio X.500.

DPC: Declaración de Prácticas de Certificación

DNTIC's: Dirección Nacional de Tecnologías de la Información y Comunicaciones

ICERT-EC: Entidad de Certificación Consejo de la Judicatura

GMT: Greenwich Mean Time

HSM (Hardware Security Module): Módulo de Seguridad Criptográfica

INOCAR: INstituto **OC**eanográfico de la **AR**mada

LDAP: Lightweight Directory Access Protocol

O (Organization) Organización: Atributo del DN de un objeto dentro de la estructura de directorio X.500.

OCSP (Online Certificate Status Protocol): Protocolo de Estatus de Certificados en línea

OID (Object Identifier): Identificador de Objetos

OU (Organizational Unit) Unidad Organizativa: Atributo del DN de un objeto dentro de la estructura de directorio X.500.

PAdES: PDF Advanced Electronic Signature

PAdES-LTV: PAdES Long Term Validation

PC: Política de Certificados

PKCS (Public Key Cryptography Standard): Estándares de Criptografía de Clave Pública

PKI (Public Key Infrastructure): Infraestructura de Clave Pública

RA (Registration **A**uthority**):** Autoridad de Registro (AR)

RFC (Request for Comments): Petición de comentarios

TSA (Time Stamping Authority): Autoridad de sellado de tiempo

TSP (Time Stamp Protocol): Protocolo de sellado de tiempo

TSS (Time-Stamping Service): Servicio de sellado de tiempo

TSQ (Time Stamp Query): Solicitud de sello de tiempo

TST (Time-Stamp Token): Token de sello de tiempo

UIT: Unión Internacional de Telecomunicaciones

UTC (Universal Time Coordinated): Hora Universal Coordinada

Código	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-14-A.05-DEC2.1-2Declaración de Prácticas de Certificación Sellado de Tiempo	Declaración de Prácticas de Certificación Sellado de Tiempo Versión 2.0	Octubre 2014	septiembre 2016

4. Conceptos generales

4.1. Servicio de Sellado de Tiempo (TSS)

El servicio de sellado de tiempo que proporciona la ICERT-EC lo constituye el sistema de generación y emisión de sellos de tiempo y su sistema de control, monitorización y supervisión de la emisión de sellos de tiempo.

4.2. Autoridad de Sellado de Tiempo (TSA)

La Autoridad de Sellado de Tiempo es la encargada de la emisión de sellos de tiempo a través del protocolo TSP conforme al estándar RFC-3161.

4.3. Comunidad de usuarios y ámbito de aplicación

4.3.1. Suscriptor

Los suscriptores son las personas físicas, organismos y entidades, ya sean públicas o privadas, que han solicitado y disponen de un token de sello de tiempo emitido por la TSA.

4.3.2. Partes que confían

Son las personas naturales o jurídicas que confían y hacen uso de los sellos de tiempo emitidos por la Autoridad de Sellado de Tiempo, TSA de la ICERT-EC, (usuarios de sellado de tiempo o suscriptores y partes que confían).

4.3.3. Ámbito de aplicación

El ámbito de aplicación de los sellos de tiempo está restringido a la comprobación de la existencia de un dato en un momento determinado de tiempo.

Código	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-14-A.05-DEC2.1-2Declaración de Prácticas de Certificación Sellado de Tiempo	Declaración de Prácticas de Certificación Sellado de Tiempo Versión 2.0	Octubre 2014	septiembre 2016

5. Política de sellado de tiempo

5.1. Generalidades

Mediante esta política se configuran las reglas utilizadas para la emisión y control de los tokens de sello de tiempo (TST) que garantizan el acceso a fuentes de tiempo fiables y se regula el nivel de seguridad para la TSA.

La desviación máxima para los tokens de sellado de tiempo es de un segundo.

El perfil del certificado de la TSA, utilizado en la firma de los TST, se ajusta al estándar RFC-3161.

A continuación se detallan los campos del perfil del certificado:

CERTIFICADO DE TSA CJ	
Componente	**Valor**
Campos de certificado X.509 v3 (tbsCertificate)	
version	v3
serialNumber	Número entero aleatorio de 20 bytes
signature	
algorithm	sha256withRSAEncryption
issuer	
commonName (CN)	*ENTIDAD DE CERTIFICACION ICERT-EC*[1]
organizationalUnitName (OU)	*SUBDIRECCION NACIONAL DE SEGURIDAD DE LA INFORMACION DNTICS*[1]
organizationName (O)	*CONSEJO DE LA JUDICATURA*[1]
localityName (L)	*DM QUITO*[1]
countryName (C)	*EC*
validity	
notBefore	Fecha y hora de emisión del certificado, codificado en UTCTime
notAfter	notBefore + 10 años, codificado en UTCTime
subject	
commonName (CN)	*AUTORIDAD DE SELLADO DE TIEMPO ICERT-EC*[1]
organizationalUnitName (OU)	*SUBDIRECCION NACIONAL DE SEGURIDAD DE LA INFORMACION DNTICS*[1]
organizationName (O)	*CONSEJO DE LA JUDICATURA*[1]
localityName (L)	*DM QUITO*[1]
countryName (C)	*EC*
subjectPublicKeyInfo	
algorithm-algorithm	rsaEncryption
subjectPublicKey	Clave pública RSA, con tamaño de 2048 bits
Extensiones de certificado X.509 v3 (extensions)	
authorityKeyIdentifier	
keyIdentifier	Valor en extensión subjectKeyIdentifier del certificado de CA Subordinada CJ
subjectKeyIdentifier	Hash SHA-1 de la clave pública RSA en subjectPublicKey
keyUsage (critical)	digitalSignature nonRepudiation

Código	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-14-A.05-DEC2.1-2Declaración de Prácticas de Certificación Sellado de Tiempo	Declaración de Prácticas de Certificación Sellado de Tiempo Versión 2.0	Octubre 2014	septiembre 2016

certificatePolicies	
policyIdentifier	1.3.6.1.4.1.43745.1.2.4.1.1.3
policyQualifiers	
policyQualifierId	id-qt-cps
qualifier-cPSuri	http://www.icert.fje.gob.ec/dpc/declaracion_practicas_certificacion.pdf
basicConstraints	
extKeyUsage (critical)	id-kp-timeStamping
cRLDistributionPoints	
distributionPoint-[1]	

fullName	
uniformResourceIdentifier	http://www.icert.fje.gob.ec/crl/icert.crl
authorityInfoAccess	
accessMethod	id-ad-ocsp
accessLocation – uniformResourceIdentifier	http://ocsp.icert.fje.gob.ec

[1] Codificado en utf8String

5.2. Identificación de la política de sellado de tiempo

Los identificadores de la política, incluidos en cada sello de tiempo, son los siguientes:

1.3.6.1.4.1.43745.1.2.4.1 – Políticas de Certificados – Dispositivos - TSA

1.3.6.1.4.1.43745.1.2.4.1.1 – Políticas de Certificados – Dispositivos - TSA - Hardware

1.3.6.1.4.1.43745.1.2.4.1.1.3 – Políticas de Certificados – Dispositivos- TSA – Hardware – HSM Genérico- Petición (PKCS #10)

5.3. Aplicación del sellado de tiempo

La utilización de sellos de tiempo emitidos por la ICERT-EC garantiza las transacciones y el no repudio en procesos entre ciudadanos, empresas y entidades.

Los tipos de certificado se detallan a continuación:

TSA (firma de sellos de tiempo)

- Subject: CN= ENTIDAD DE SELLADO DE TIEMPO DEL CONSEJO DE LA JUDICATURA, L=DM QUITO, OU= DNTICS, O=CONSEJO DE LA JUDICATURA, C=EC
- Sin subjectAltName
- Validez: 10 años
- Tamaño de clave pública RSA: 2048 bits (claves en HSM-P10)

Código	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-14-A.05-DEC2.1-2Declaración de Prácticas de Certificación Sellado de Tiempo	Declaración de Prácticas de Certificación Sellado de Tiempo Versión 2.0	Octubre 2014	septiembre 2016

Dispositivos de tipos de certificados de dispositivo

Tipo de certificado	Dispositivo criptográfico
RA CJ (firma de peticiones enviadas a la CA)	• HW-HSM-PKCS #10 (se genera las claves y la petición y se instala el certificado en la RA CJ)
TSA CJ (firma de sellos de tiempo)	• HW-HSM-PKCS #10 (se genera las claves y la petición y se instala el certificado en la TSA CJ)

6. Obligaciones y responsabilidades

6.1. Obligaciones de la TSA

6.1.1. Obligaciones generales

La Autoridad de Sellado de Tiempo de la ICERT-EC tiene las siguientes obligaciones:

- Cumplir las responsabilidades y obligaciones descritas en este documento y las establecidas en la DPC de la ICERT-EC y la legislación aplicable.
- Realizar las operaciones de sellado de tiempo de acuerdo a la presente política.
- Emitir sellos de tiempo de acuerdo a la información proporcionada en el momento de su emisión y libres de errores de ingreso de datos.
- Utilizar sistemas y productos fiables que garanticen la seguridad técnica y que estén protegidos mediante procesos criptográficos dentro de los procesos de certificación a los que sirven de respaldo.
- Garantizar la precisión de la fecha y la hora en que se emite un sello de tiempo.
- Hacer pública esta política así como sus versiones anteriores, si las hubiere, y los documentos relacionados a ésta en la página web de la ICERT-EC.
- Emitir sellos de tiempo que cumplen las especificaciones de la RFC - 3161 con una precisión de un segundo.
- Garantizar que los procedimientos y prácticas relacionadas con la emisión de tokens de sellado de tiempo cumplen lo establecido en los documentos técnicos, operacionales y de procedimientos de la ICERT-EC.

Información adicional sobre las obligaciones de la ICERT-EC constan en la Declaración de Prácticas de Certificación DPC.

6.1.2. Obligaciones de la TSA hacia los suscriptores

- Utilizar una fuente fiable de tiempo.
- Utilizar sistemas para la provisión de servicios de sellado de tiempo que cumplan lo contemplado en la normativa técnica vigente.
- Incluir un número de serie único para cada token de sello de tiempo generado.
- Producir un token de sello de tiempo una vez que se reciba una solicitud válida de un suscriptor, cuando esto sea posible.
- Incluir en cada token de sello de tiempo un identificador que indique la política de seguridad bajo la cual fue creado.
- Garantizar el acceso permanente a los servicios de sellado de tiempo que proporciona, excluyendo los tiempos mínimos de suspensión requeridos para el mantenimiento de los sistemas y equipos.
- Notificar a los suscriptores del servicio acerca de las interrupciones del servicio debidas a mantenimiento, planificadas con antelación, utilizando los medios de difusión disponibles.
- No utilizar datos personales en los tokens de sello de tiempo generados.
- Firmar cada mensaje de sello de tiempo con una clave reservada específicamente para ese propósito.

6.2. Obligaciones de los suscriptores

Es obligación de los suscriptores del servicio previa la utilización de un sello de tiempo:

- Verificar que los Sellos Digitales de Tiempo (TST) han sido emitidos de manera adecuada por la Autoridad de Sellado de Tiempo (TSA).
- Verificar la firma electrónica de la ICERT-EC y comprobar en la Lista de Certificados Revocados, CRL, el estado del certificado de la TSA.

La CRL puede consultarse en la siguiente dirección: http://www.icert.fje.gob.ec/crl/icert.crl

También puede consultarse el servicio OCSP disponible en: http://ocsp.icert.fje.gob.ec para comprobar la validez del certificado de la TSA.

6.3. Obligaciones de las partes que confían

- Cumplir las obligaciones establecidas en la presente DPC - ST y las impuestas por la normativa vigente.
- Asumir la responsabilidad derivada de la utilización de un TST sin observar el debido cuidado.
- Verificar la firma del sello de tiempo.
- Comprobar el estado del certificado de la ICERT-EC y su período de vigencia.
- Verificar que el número de serie del certificado de la TSA no se encuentra en la CRL.

Código	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-14-A.05-DEC2.1-2Declaración de Prácticas de Certificación Sellado de Tiempo	Declaración de Prácticas de Certificación Sellado de Tiempo Versión 2.0	Octubre 2014	septiembre 2016

7. Requisitos en materia de prácticas de TSA

La TSA implementa los controles necesarios para cumplir los siguientes requerimientos en función de garantizar los objetivos de seguridad y de confidencialidad del servicio.

7.1. Declaración y difusión de prácticas

7.1.1. Declaración de prácticas de la TSA

- Garantizar la confiabilidad necesaria para proveer servicios de sellado de tiempo.
- Realizar los controles de seguridad y procedimientos operacionales necesarios para prevenir amenazas a las inversiones y negocios.
- Los sellos de tiempo emitidos están firmados con la clave privada correspondiente al certificado de firma de sellos de tiempo de la TSA.
- Entre los procedimientos de seguridad y operacionales de uso interno de la TSA en la ICERT-EC constan:
  - Política de seguridad
  - Política de archivo
  - Política de auditoría
  - Política de copias
  - Política de gestión del cambio.

7.1.2. Declaración de divulgación de prácticas de la TSA

La prestación del servicio de sellado de tiempo se realiza en base a la RFC3161 “HTTP Time-Stamp Protocol via HTTP”. El servicio toma al momento temporal de su reloj interno, sincronizado con la hora oficial del Ecuador y genera una marca temporal. Esta marca temporal viene firmada por el certificado de la TSA, lo cual le otorga garantías de autenticidad e integridad.

La Autoridad de Sellado de Tiempo se comunica con la base de datos donde se almacenan los datos sobre los sellos de tiempo emitidos y con una fuente fiable de tiempo en red NTP para sincronizar la hora a intervalos regulares.

El servicio de sellado de tiempo está disponible de forma ininterrumpida todos los días del año, permitiendo en todo momento su consumo en línea.

7.2. Gestión del ciclo de vida de las claves

7.2.1. Generación de claves de la TSA

La generación de claves de la TSA se realiza en el HSM por personal autorizado y calificado por la ICERT-EC. Estas claves se guardan cifradas con clave maestra.

El algoritmo de la clave pública es RSA Encryption y el tamaño de la clave pública es de 2048 bits, según lo descrito en numeral 5.1 de este documento.

7.2.2. Protección de la clave privada de la TSA

La clave privada de la TSA se archiva en el en el HSM como se explica en el numeral anterior y su acceso es multipersona.

7.2.3. Difusión de la clave pública de la TSA

El certificado de la TSA, que incluye su clave pública, puede encontrarse en la página web de la ICERT-EC.

7.2.4. Regeneración de la clave de la TSA

En caso de compromiso de la clave de la TSA o cuando ha expirado el certificado y sus claves, y si ésta debe ser revocada, la nueva clave será generada con una ceremonia de generación cumpliendo los requisitos establecidos para ser suministrada a los usuarios.

7.2.5. Destrucción de la clave privada de la TSA

La destrucción de la clave privada es un procedimiento interno.

7.2.6. Gestión de los HSM

La gestión de los HSM cumple los parámetros establecidos por los fabricantes para garantizar su seguridad y confiabilidad. Los procedimientos de manejo de los HSM constituyen información de uso interno.

El Módulo de Hardware Criptográfico HSM tiene certificación de seguridad FIPS 140-2 Nivel 3 y/o Common Criteria EAL4+.

7.3. Sellado de tiempo

7.3.1. Token de Sello de Tiempo (TST)

Los token de sello de tiempo TST emitidos por la TSA de la ICERT-EC incluyen un identificador único de política según lo descrito en el numeral 5.2 y el identificador de la presente DPC-ST a la que están sujetos.

Los sellos de tiempo incluyen valores de fecha y hora. La hora de los equipos de la TSA se sincronizará con la hora de los equipos del servidor NTP INOCAR como hora legal en el Ecuador a través de su servicio NTP.

La generación de los token de sello de tiempo se realiza según lo descrito en el RFC-3161 que describe el formato de una solicitud enviada a una TSA y de la respuesta que se devuelve.

7.3.2. Sincronización del reloj con UTC

Para garantizar la exactitud del tiempo en los sellos de tiempo el servicio NTP de los equipos de la TSA procesa las peticiones NTP de sincronización de hora.

7.4. Operación y gestión de la TSA

Los controles relativos a la seguridad en la operación y gestión de la TSA se rigen a lo establecido en la DPC y que tienen relación con:

- Control de riesgos
- Seguridad del personal
- Seguridad física
- Procedimientos
- Gestión de acceso a los sistemas

7.4.1. Compromiso de los servicios de sellado de tiempo

En caso de compromiso de los servicios de sellado de tiempo se procederá de acuerdo a lo previsto en la política de continuidad del servicio de la ICERT-EC.

7.4.2. Cese de la TSA

De producirse el cese de la TSA se garantiza la ejecución de los procedimientos para ocasionar la mínima afectación a los suscriptores. Se deberá cumplir entre otras, las siguientes actividades:

- Comunicar al Organismo de Control el cese de la actividad y los mecanismos establecidos para garantizar la validez de los sellos existentes.
- Transferir la gestión de emisión de sellos de tiempo, previo el consentimiento de los suscriptores, a otra entidad de certificación y servicios relacionados, habiéndolo comunicado previamente al organismo de control.

7.4.3. Cumplimiento de los requisitos legales

La ICERT-EC como Autoridad de Sellado de Tiempo cumple con la normativa legal vigente sobre la materia.

7.4.4. Registro de información relativa a la operación de la TSA

Los registros de la creación de sellos de tiempo y el control de la operación de la TSA se guardan temporalmente en ficheros locales que luego se guardan en la base de datos del componente.

7.5. Esquema organizativo

La Autoridad de Sellado de Tiempo AST forma parte de la arquitectura lógica de los componentes de la infraestructura PKI de la ICERT-EC con sus correspondientes elementos de software específicos para su operación.

7.6. Requisitos comerciales y legales

7.6.1. Tarifas

7.6.1.1. Tarifas de emisión de sellos de tiempo

Las tarifas por emisión de sellos de tiempo se publican en la página web del Consejo de la Judicatura en la siguiente ubicación: http://www.icert.fje.gob.ec sección tarifas.

7.6.1.2. Tarifas de acceso a los sellos de tiempo

No existe una tarifa para el acceso a la información de los sellos de tiempo emitidos por la ICERT-EC.

7.6.1.3. Tarifas de acceso a la información de estado o revocación

No existe una tarifa para el acceso a la información publicada acerca del estado de los certificados que firman los sellos de tiempo emitidos por la ICERT-EC.

7.6.1.4. Tarifas por otros servicios

Las tarifas por otros servicios se encuentran publicadas en la página web de la ICERT-EC.

7.6.2. Responsabilidad financiera

La ICERT-EC mantiene una póliza de responsabilidad civil para responder ante cualquier eventualidad que signifique un perjuicio para los suscriptores, siempre y cuando los daños y perjuicios se deriven de errores, omisiones o actos negligentes por parte de la ICERT-EC.

Se aclara que la ICERT-EC no se responsabiliza por actos relacionados con el incumplimiento o ejecución incorrecta de las obligaciones contraídas por el suscriptor y/o usuario de un sello de tiempo, y por la incorrecta utilización de los certificados digitales y claves privadas.

7.6.3. Notificaciones

Todas las notificaciones se harán según lo establecido en la DPC de la ICERT-EC.

Los correos que se envíen a los suscriptores del servicio de sellado de tiempo serán firmados digitalmente.

7.6.4. Modificaciones

Según lo especificado en la DPC de la ICERT-EC.

7.6.5. Resolución de controversias

Según lo especificado en la DPC de la ICERT-EC.

7.6.6. Legislación aplicable

Según lo especificado en la DPC de la ICERT-EC.