



Declaración de Prácticas y Política de Sellado de Tiempo (Timestamping, TSA)

OID 2.16.484.101.10.316.2.4.1.3.1.1.3(*)

()El nuevo OID 2.16.484.101.10.316.2.4.1.3.1.1.3 es equivalente al anterior 2.16.484.101.10.316.1.4.1.3.1.0.1.3, se cambia por error en la codificación de la SE*

Título del documento:	Práctica y Política de sellado de tiempo (Timestamping, TSA)
Nombre del fichero:	06B_ACEDICOMMX-PracticasYPoliticaServicioTimestamping.doc
Versión:	1.3.1
Estado:	VIGENTE
Fecha:	14/01/10
Autor:	JOSE VILATA


Revisión, Aprobación		
Revisado por:	Jose Vilata, Raul Sant.	Fecha: 28/10/09
Aprobado por:	Jose Vilata	Fecha: 28/10/09

Historial de cambios			
Versión	Fecha	Descripción de la acción	Páginas
1.0	15/10/08	Documento inicial	
1.1	11/02/09	Se introducen apartado de prácticas y otras modificaciones a petición de la Secretaría de Economía	
1.2	28/10/09	Modificaciones solicitadas por SE en oficio 316.09.002326	
1.2	28/10/09	Modificaciones solicitadas por SE en oficio 316.09.002326	
1.3	14/01/10	Modificaciones solicitadas por SE en oficio 316.09.002774	
1.3.1	12/7/2010	Cambio de OID a petición de la SE por error en la codificación. El nuevo OID 2.16.484.101.10.316.2.4.1.3.1.1.3 es equivalente al anterior 2.16.484.101.10.316.1.4.1.3.1.0.1.3	

Tabla de Contenidos

1 INTRODUCCIÓN.....	6
2 REFERENCIAS	7
3 DEFINICIONES Y ABREVIATURAS	8
3.1. DEFINICIONES	8
3.2. ABREVIATURAS	8
4 CONCEPTOS GENERALES.....	9
4.1 SERVICIO DE SELLADO DE TIEMPO	9
4.2. AUTORIDAD DE SELLADO DE TIEMPO (TSA)	10
4.3. SUSCRIPTORES	10
5. POLÍTICA DE SELLADO DE TIEMPO	11
5.1. VISTA GENERAL	11
5.2. IDENTIFICACIÓN DE LA POLÍTICA Y PRÁCTICAS DE SELLADO DE TIEMPO	11
5.3. APLICACIÓN DEL SELLADO DE TIEMPO	12
6 OBLIGACIONES Y RESPONSABILIDADES	13
6.1 OBLIGACIONES DE LA TSA.....	13
6.1.1 <i>Obligaciones a los suscriptores</i>	13
6.1.2 <i>Responsabilidad financiera</i>	13
6.1.3 <i>Exoneración de responsabilidad</i>	14
6.2 OBLIGACIONES DE LOS SUSCRIPTORES	14
6.3 OBLIGACIONES DE LAS PARTES CONFIANTES	15
7 PRÁCTICAS DE SELLADO DE TIEMPO.....	16
7.1 INTRODUCCIÓN	16
7.2 GESTIÓN DEL CICLO DE VIDA DE LAS CLAVES	16
7.2.1. <i>Generación de claves de la TSA</i>	16
7.2.2. <i>Protección de la clave privada de la TSA</i>	16
7.2.3 <i>Publicación del certificado de TSA</i>	17
7.2.3 <i>Cambio de certificado de TSA</i>	17
7.2.5. <i>Destrucción de la clave privada de la TSA</i>	17
7.2.6. <i>Gestión de los HSM</i>	17
7.3 SELLADO DE TIEMPO	17
7.3.1. <i>Token de sello de tiempo</i>	17
7.3.2. <i>Sincronización del reloj con UTC</i>	18
7.4 IMPLEMENTACIÓN DE LA SOLICITUD Y RESPUESTA DE SELLOS DE TIEMPO.....	19
7.4.1. <i>Protocolo Timestamp vía HTTP</i>	19
7.4.2 FORMATO DE LOS MENSAJES	19
7.4.2.1 <i>Timestamp Request</i>	19
7.4.2.2 <i>Timestamp Response</i>	20
7.4.2.3 <i>Validate Request</i>	22
7.4.2.4 <i>Validate Reply</i>	23
7.5. OPERACIÓN Y GESTIÓN DE LA TSA	23
7.5.1. <i>Gestión de la seguridad</i>	23
7.5.2. <i>Control de riesgos e inventario de activos</i>	23
7.5.3. <i>Seguridad del personal</i>	23

7.5.4. Seguridad física	23
7.5.5. Gestión de las operaciones	24
7.5.6. Gestión de acceso a los sistemas	24
7.5.7. Mantenimiento y despliegue de sistemas de confianza	24
7.5.8. Compromiso de los servicios de sellado de tiempo.	24
7.5.9 Cese de la actividad de la TSA	25
7.5.10. Cumplimiento de los requisitos legales	25
7.5.11. Registro de información relativa a la operación del servicio de sellado de tiempo	25
8 PROTECCIÓN DE DATOS PERSONALES	26
8.1.PLAN DE PROTECCIÓN DE DATOS PERSONALES.....	26
8.2.PROCEDIMIENTOS DE PROTECCIÓN DE CONFIDENCIALIDAD DE LA INFORMACIÓN.....	26
8.3.INFORMACIÓN CONSIDERADA PRIVADA.....	26
8.4.INFORMACIÓN NO CONSIDERADA PRIVADA.	27
8.5.RESPONSABILIDADES.	27
8.6.PRESTACIÓN DEL CONSENTIMIENTO EN EL USO DE LOS DATOS PERSONALES.	27
8.7.COMUNICACIÓN DE LA INFORMACIÓN A AUTORIDADES ADMINISTRATIVAS Y/O JUDICIALES.	27
9. RESOLUCIÓN DE CONFLICTOS.....	27
9.1.RESOLUCIÓN EXTRAJUDICIAL DE CONFLICTOS.	27
9.2.JURISDICCIÓN COMPETENTE.	28
10.LEGISLACIÓN APLICABLE.....	28

	PRÁCTICAS Y POLITICA DE SELLADO DE TIEMPO (TIMESTAMPING)	
	Edición 1.3	Página 6

1 Introducción

EDICOM, como Prestador de Servicios de Certificación que emite certificados reconocidos por la Secretaría de Economía de México (SE), también ha sido homologado para ofrecer otros servicios adicionales y, entre ellos, el servicio de Sellado de Tiempo.

Este documento describe las Prácticas y la Política de Sellado Digital de Tiempo (Timestamping) de la ACEDICOMMX y establece las reglas generales empleadas por la Autoridad de Sellado de Tiempo de la Autoridad de Certificación de EDICOM México (en adelante TSA de la ACEDICOMMX), para la emisión de tokens que contienen sellos de tiempo firmados. Se establecen en este documento los participantes de estos procesos, especificando sus responsabilidades, derechos y ámbito de aplicación.

La legislación mexicana, en concreto en las “Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación” publicadas en el DOF el 10 de agosto de 2004, recoge la emisión de sellos de tiempos indicando lo siguiente en su regla 7.2:


(REGLA 7.2. MODIFICADA DOF 05 03 07)

El sistema de sellos digitales de tiempo deberá cumplir, en todo momento, por lo menos, con el estándar internacional Internet X.509 “Public Key Infrastructure Time Stamp” y considerar los RFC 3161 y 3628, o los que lo suplan, previo aviso que la Secretaría haga por escrito a los Prestadores de Servicios de Certificación.

Sin embargo, es intención de EDICOM dotar a los sellos de tiempo emitidos la condición de “Sellos de Tiempo reconocidos” equivalente a la condición de “Firmas electrónicas fiables”, en la medida que esto sea posible y comprometiéndose a cumplir con la legislación aplicable en cada caso. El término “sello de tiempo reconocido” es mas un término comercial que legal ya que trata de transmitir fiabilidad tanto del prestador de servicio como fiabilidad y garantía del propio servicio de emisión de sellos digitales de tiempo por el hecho de haber pasado el proceso de certificación oficial de la secretaría de Economía.

La presente declaración de prácticas y política de Timestamping es conforme a la norma del ETSI TS 102 023 v1.2.1 “Policy requirements for time-stamping authorities” y a su especificación equivalente RFC-3628 “Requirements for time-stamping authorities”.

Se asume cierto grado de conocimiento por parte del lector de conceptos relacionados con las infraestructuras de clave pública y los sellos de tiempo. Si este no fuera el caso, se recomienda al lector que se informe sobre los temas anteriores antes de continuar con la lectura del presente documento.

	PRÁCTICAS Y POLITICA DE SELLADO DE TIEMPO (TIMESTAMPING)	
	Edición 1.3	Página 7


El presente documento puede ser usado por las partes confiantes y los subscriptores de los servicios proporcionados por la TSA de la ACEDICOMMX como base para garantizar la confianza de los servicios que se describen en este documento.

Esta política esta basada en criptografía de clave pública, fuentes de tiempo fiables y certificados X.509 v3 y está subordinada al cumplimiento de las Condiciones Generales expuestas en la **Declaración de Prácticas de Certificación (CPS)** de la ACEDICOMMX.

2 Referencias

Los documentos que se citan a continuación se mencionan a lo largo del texto:

- [1] Declaración de Prácticas de Certificación de la ACEDICOMMX (CSP)
- [2] ETSI TS 102 023 “Policy Requirements for time-stamping authorities”
- [3] RFC-3161 “Internet X.509 Public Key Infrastructure – Time Stamp Protocol (TSP)”
- [4] ETSI TS 101 861 “Time Stamping Profile”
- [5] ETSI SR 002 176 “Algorithms and Parameters for Secure Electronic Signatures”
- [6] Procedimiento Operativo de Generación de Claves de la CA (ACEDICOMMX)
- [7] Plan de Administración de claves de la CA (ACEDICOMMX)

	PRÁCTICAS Y POLITICA DE SELLADO DE TIEMPO (TIMESTAMPING)	
	Edición 1.3	Página 8

3 Definiciones y abreviaturas

3.1. Definiciones

Para los propósitos del presente documento, se aplican los siguientes términos y definiciones:

- **Autoridad de Sellado de Tiempo:** Sistema de emisión y gestión de sellos de tiempo seguros
- **Subscriber:** Persona o entidad que solicita los servicios proporcionados por la Autoridad de Sellado de Tiempo.
- **Token de sello de tiempo:** Dispositivo de datos empleado en un proceso de creación de firma electrónica, que une la representación de un dato a un tiempo concreto, estableciendo así evidencia de que el dato existía antes de ese tiempo.
- **Usuario:** Destinatario de un Token de sello de tiempo y que confía en el mismo.
- **Declaración de Prácticas de sellado de tiempo:** Declaración de las Prácticas que una Autoridad de sellado de tiempo emplea en la emisión.

3.2. Abreviaturas

TSA: Autoridad de Sellado de Tiempo
TSS: Servicio de sellado de tiempo
TSQ: Solicitud de sello de tiempo
ACEDICOMMX: Autoridad de Certificación de EDICOM
TST: Token de sello de tiempo
IETF: Internet Engineering Task Force
CEN: Comité Europeo de Normalización
CWA: Cen Workshop Agreement
RFC: Request for comment
UTC: Universal Time Coordinated
CRL: Certificate Revocation List
FIPS: Federal Information Processing Standards
HSM: Hardware Security Module
GPS: Global Positioning System

4 CONCEPTOS GENERALES

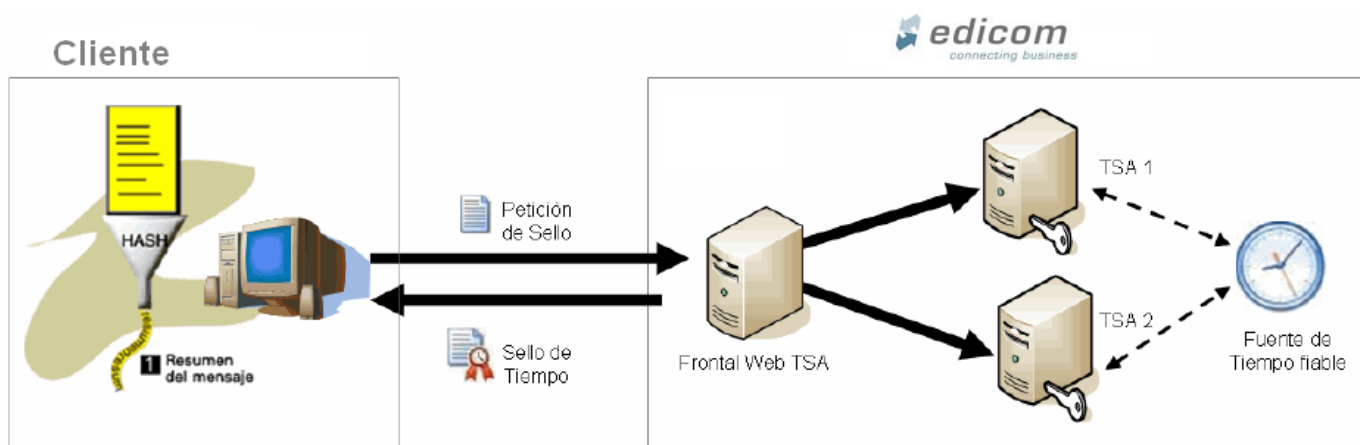
4.1 Servicio de sellado de tiempo


El sellado de tiempo (Timestamping) es un mecanismo on-line que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo.

La implementación de la política de sellado de tiempo se debe cumplir con el protocolo definido en la norma **RFC 3161 “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)”**.

Los pasos para generar un sello de tiempo son los siguientes:

- El cliente calcula el hash del documento a sellar
- El cliente envía una solicitud de sello de tiempo a una URL determinada de ACEDICOMMX siguiendo el protocolo RFC 3161, incluyendo el hash del documento a sellar
- ACEDICOMMX recibe la petición, revisa si la petición está completa y correcta y realiza un control de acceso en función del usuario y password del cliente.
- Si el resultado es correcto, la TSA firma la petición generando un Sello de Tiempo (incluyendo el hash del documento, la fecha y hora obtenida de una fuente fiable y la firma electrónica de la TSA).
- El sello de tiempo se envía de vuelta al Cliente
- El Cliente debe validar la firma del sello y custodiarlo debidamente
- La TSA de la ACEDICOMMX también mantendrá un registro de los sellos emitidos para su futura verificación si así se ha contratado con el cliente



	PRÁCTICAS Y POLITICA DE SELLADO DE TIEMPO (TIMESTAMPING)	
	Edición 1.3	Página 10

4.2. Autoridad de Sellado de Tiempo (TSA)

La autoridad en la que confían los usuarios de los servicios de sellado de tiempo (suscriptores y partes confiantes) para la emisión de los sellos de tiempo. La TSA tiene responsabilidad global en la provisión del servicio de sellado de tiempo que se identifica en la cláusula 4.1.

4.3. Suscriptores

Los suscriptores de este servicio son los usuarios del sistema con los que se haya suscrito el correspondiente convenio de prestación de servicios de sellado de tiempo electrónico.

Los clientes envían peticiones de sellado y reciben sellos de tiempo siguiendo el protocolo RFC3161 Time Stamp Protocol (TSP).

Los clientes deben adaptar sus sistemas para poder realizar peticiones de sellado de tiempo. Existen librerías públicas que implantan el protocolo TSP en diversos lenguajes de programación:

- **BouncyCastle** (<http://www.bouncycastle.org>): Conjunto de librerías criptográficas que implementan el protocolo TSP en los lenguajes Java y C#
- **OpenTSA** (<http://www.opentsa.org>): Es una ampliación de la librería criptográfica OpenSSL que implementa el protocolo TSP en lenguaje C.
- **Digistamp** (<http://digistamp.com/toolkitDoc/MSToolKit.htm>): Toolkit basado en la librería criptográfica CryptoAPI de Microsoft que implementa el protocolo TSP en Visual Basic
- **IAIK**: Incluye librerías criptográficas en Java que implementan el protocolo TSP. Estas librerías son gratuitas únicamente para propósitos no comerciales
- **Adobe Reader**: La aplicación Adobe Reader 8 permite validar sellos de tiempo incluidos en documentos PDF.

5. Política de Sellado de Tiempo

5.1. Vista general

La presente política establece el conjunto de reglas utilizadas durante la emisión y el control de los tokens de sello de tiempo (TST), y regulan además el nivel de seguridad para la TSA.

Los tokens de sellado de tiempo son emitidos con una desviación máxima de 500ms.


El perfil del certificado de la TSA, utilizado en la firma de los TST, se ajusta a lo especificado por el IETF en RFC-3161. En la siguiente tabla se detallan los campos básicos de este perfil:

Versión	v3	S		F
Serial Number	7F6A783DE9C70E0E	S		F
Signature Algorithm	SHA1withRSAEncryption	S		F
Issuer Distinguished Name	CN=ACEDICOMMX Servidores,OU=PKI,O=EDICOM,C=MX	S		F
Validez	10 años	S		F
Subject Public Key Info	Tipo de clave: RSA Longitud de la clave: 2048 bits	S		F
Subject		S		D
CommonName (CN)	ACEDICOMMX TSA	S		D
Organization Unit (OU)	PKI	S		D
Organization (O)	EDICOM	S		D
Country (C)	MX	S		D
SubjectKeyIdentifier	E3:CB:B2:FF:06:9F:3C:D6:37:A7:AD:6F:8B:93:61:43:B8:5A:79:81	S		D
AuthorityKeyIdentifier	Keyid:AD:C1:E8:40:30:96:01:16:52:02:41:38:3D:B6:51:F3:9E:82:46:4B	S		F
BasicConstraints		S	X	F
CA	Falso	S	X	F
pathLength	No aplicable (0)			F
KeyUsage	digitalSignature	S	X	F
ExtendedKeyUsage	TimeStamping	S	X	F

La TSA que proporciona sus servicios bajo la estructura de la ACEDICOMMX, emite los sellos de tiempo acorde a la recomendación ETSI TS 101 861. Cada sello de tiempo incluye el identificador de la política, descrito en el capítulo 5.2 “Identificación de la política y prácticas de sellado de tiempo”, de la presente política.

El servicio de Sellado de Tiempo es accesible vía http en la dirección **tsa.acedicom.edicomgroup.com** por el puerto 9026 y 9027 (https). La URL a definir en el cliente **<http://tsa.acedicom.edicomgroup.com:9026>** o **<https://tsa.acedicom.edicomgroup.com:9027>**.

5.2. Identificación de la política y prácticas de sellado de tiempo

	PRÁCTICAS Y POLÍTICA DE SELLADO DE TIEMPO (TIMESTAMPING)	
	Edición 1.3	Página 12

La información de la política y prácticas, que controla la emisión y el control de los tokens de sellado de tiempo, esta definida en la siguiente Tabla :

Nombre del documento	Prácticas y Política de sellado de tiempo de la ACEDICOMMX
Versión del documento	1.3.1
Estado del documento	Vigente
OID (Object Identifier)	2.16.484.101.10.316.2.4.1.3.1.1.3(*)
Fecha de emisión	15 de Octubre de 2008
Fecha de expiración	No aplicable.
Localización	http://acedicom.edicomgroup.com/mx

(*) El nuevo OID 2.16.484.101.10.316.2.4.1.3.1.1.3 es equivalente al anterior 2.16.484.101.10.316.1.4.1.3.1.0.1.3, se cambia por error en la codificación de la SE.

El identificador de las prácticas y política de la Autoridad de Sellado de Tiempo de la ACEDICOMMX esta incluido en cada sello de tiempo. También aparece en el documento de Declaración de Términos y Condiciones de Uso de la Autoridad de Sellado de Tiempo.

5.3. Aplicación del sellado de tiempo

5.3.1. Usos permitidos


Los sellos de tiempo emitidos por la Autoridad de Sellado Digital de Tiempo de la ACEDICOMMX pueden emplearse para garantizar las transacciones y el no repudio en procesos en los cuales intervenga cualquier organismo o entidad con los que se haya formalizado un contrato de emisión de Sellos Digitales de Tiempo.

5.3.2. Usos prohibidos

Los sellos de tiempo emitidos por la TSA ACEDICOMMX se utilizarán únicamente conforme a la función y finalidad que tengan establecida en la presente Declaración de Prácticas y Política de TimeStamping, y con arreglo a la normativa vigente.

La contratación de los sellos de tiempo de la TSA ACEDICOMMX admite solamente el uso en el ámbito de actividad del SOLICITANTE o de la entidad a la que está vinculado.

En todo caso, los sellos de tiempo de la TSA ACEDICOMMX no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieran actuaciones a prueba de errores, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un error pudiera directamente comportar la muerte, lesiones personales o daños medioambientales severos.

	PRÁCTICAS Y POLÍTICA DE SELLADO DE TIEMPO (TIMESTAMPING)	
	Edición 1.3	Página 13

6 OBLIGACIONES Y RESPONSABILIDADES

6.1 Obligaciones de la TSA

6.1.1 Obligaciones a los subscriptores


ACEDICOMMX, actuando como Autoridad de Sellado de Tiempo (TSA) se obliga a:

- Respetar lo dispuesto en esta Política de Sellado de Tiempo.
- Proteger sus claves privadas de forma segura.
- Emitir sellos de tiempo conforme a esta Política y a los estándares de aplicación.
- Garantizar que la hora y fecha incluidas en los sellos se mantienen dentro de los márgenes precisión establecida en el contrato entre el cliente y ACEDICOMMX, que en ningún caso pueden ser superiores a lo establecido en el apartado 5.1.
- Emitir sellos de tiempo según la información enviada por el cliente y libres de errores de entrada de datos.
- Emitir sellos de tiempos cuyo contenido mínimo sea el definido por la normativa vigente, cuando sea aplicable.
- Publicar esta Política de Sellado de Tiempo
- Informar sobre las modificaciones de la Política de Sellado de Tiempo a clientes y terceros que confían en los sellos de tiempo.
- Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida, destrucción o falsificación.
- Custodiar los sellos de tiempo emitidos para los clientes que contraten el servicio de custodia
- ACEDICOMMX, en su actividad de prestación de servicios de certificación, responderá por el incumplimiento de lo establecido en esta Política de Sellado de Tiempo y, allí donde sea aplicable, por lo que dispone la Ley 59/2003, de 19 de diciembre, de firma electrónica o su normativa de desarrollo.

Sin perjuicio de lo anterior ACEDICOMMX no garantizará los algoritmos y estándares criptográficos utilizados ni responderá de los daños causados por ataques externos a los mismos, siempre que hubiere aplicado la diligencia debida según el estado de la técnica en cada momento, y hubiere actuado conforme a lo dispuesto en las presentes Políticas de TSA y en la legislación vigente, donde sea aplicable.

6.1.2 Responsabilidad financiera

La estipulada para la Autoridad de Certificación, es decir, la Autoridad de Sellado Digital de Tiempo de la ACEDICOMMX, en su actividad como prestador de servicios de Certificación dispone de recursos económicos suficientes para afrontar el riesgo de la responsabilidad por daños y perjuicios

	PRÁCTICAS Y POLÍTICA DE SELLADO DE TIEMPO (TIMESTAMPING)	
	Edición 1.3	Página 14

ante los usuarios de sus servicios y a terceros, no obstante su responsabilidad en el ejercicio de la actividad de PSC tal como se define en la legislación a los efectos del artículo 102, inciso A), fracción V, del Código de Comercio, y del apartado 2.bis., de las Reglas Generales para los PSC de 10 de agosto de 2004, en relación con el artículo 89 del Código de Comercio por las que se describen las condiciones a las que se sujetará la fianza que otorguen los solicitantes que obtengan su acreditación como PSC, queda garantizada mediante un Seguro de Responsabilidad Civil Profesional con una cobertura de Tres millones de Euros (3.000.000 €).

6.1.3 Exoneración de responsabilidad

ACEDICOMMX no será responsable en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:


- Estado de Guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por el Cliente o por los Terceros, o cualquier otro caso de fuerza mayor.
- Por el uso indebido o fraudulento de los sellos de tiempo.
- Por el uso indebido de la información contenida en el Certificado o en la CRL.
- Por el contenido de los mensajes o documentos sellados.
- En relación a acciones u omisiones del Cliente
- Falta de veracidad de la información suministrada para emitir el sello
- Negligencia en la conservación de sus datos de acceso al servicio de sellado de tiempo, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
- Extralimitación en el uso del sello de tiempo, según lo dispuesto en la normativa vigente y en la presente Política de TSA
- En relación a acciones u omisiones del Usuario, tercero que confía en el certificado:
- Falta de comprobación de la suspensión o pérdida de vigencia del certificado electrónico de la TSA publicada en el servicio de consulta sobre la vigencia de los certificados o falta de verificación de la firma electrónica.

6.2 Obligaciones de los suscriptores

El Cliente estará obligado a cumplir con lo dispuesto por la normativa y además a:

- Respetar lo dispuesto en los documentos contractuales firmados con la TSA.
- Verificar la corrección de la firma digital del sello de tiempo y la validez del certificado de la TSA en el momento de firmarlo.

Obligaciones adicionales pueden encontrarse en la CSP [1], capítulo 2.1.3, "Obligaciones de los suscriptores"


 edicom <i>connecting business</i>	PRÁCTICAS Y POLITICA DE SELLADO DE TIEMPO (TIMESTAMPING)		
		Edición 1.3	Página 15

6.3 Obligaciones de las partes confiantes

Será obligación de los Usuarios cumplir con lo dispuesto por la normativa vigente y además:

- Verificar la corrección de la firma del sello de tiempo y la validez del certificado de la TSA en el momento de firmarlo.

Obligaciones adicionales pueden encontrarse en la CSP [1], capítulo 2.1.4, “Obligaciones de las partes confiantes”

	PRÁCTICAS Y POLITICA DE SELLADO DE TIEMPO (TIMESTAMPING)		Edición	Página
			1.3	16

7 PRÁCTICAS DE SELLADO DE TIEMPO

7.1 INTRODUCCIÓN

Las prácticas de sellado de tiempo detallan la implementación de los controles necesarios para garantizar la fiabilidad y confianza del servicio.

Se detallan los mecanismos y procedimientos establecidos para el cumplimiento de lo establecido en el capítulo 6, “Obligaciones y responsabilidades”, del presente documento, que constituyen las bases del funcionamiento de la TSA.

Los elementos para contactar con los responsables, se detallan en la CPS [1], capítulo 1.4 “Datos de contacto”.

7.2 GESTIÓN DEL CICLO DE VIDA DE LAS CLAVES

7.2.1. Generación de claves de la TSA

Las claves de la TSA se generan en módulo de seguridad hardware (en adelante HSM), que cumple con el estándar NIST FIPS 140-2 nivel 3, por personal autorizado de la ACEDICOMMX. La descripción de los roles y controles del personal puede encontrarse en la CPS[1]1, en el apartados 5.2 “Controles Procedimentales” [1]. Para más detalle puede revisar el procedimiento operativo “Generación de claves de la CA”[6] y el “Plan de Administración de claves”[7].

El entorno de generación de las claves cumple los requisitos normativos impuestos por la ACEDICOMMX, de acuerdo con la CPS[1] y cumplen con los requerimientos descritos en ISO 15408 (Information technology. Security techniques. Evaluation criteria for IT security).


El algoritmo y tamaño de claves se describen en el capítulo 5.1 “Vista general” de esta política, cumpliendo lo referenciado por ETSI SR 002 176.

7.2.2. Protección de la clave privada de la TSA

Los niveles de seguridad del HSM donde se almacena la clave se describen en el capítulo 7.2.1 “Generación de la clave de la TSA” de esta política.

Esta clave se encuentra bajo control multipersonal. Se encuentra dividida en varios fragmentos y es necesario un mínimo de dos de estos fragmentos para recomponer la clave.

Las copias de Backup de la clave privada se almacenan cifradas en archivos seguros ignífugos.

	PRÁCTICAS Y POLÍTICA DE SELLADO DE TIEMPO (TIMESTAMPING)	
	Edición 1.3	Página 17

7.2.3 Publicación del certificado de TSA

El certificado de la TSA, que incluye su clave pública, se distribuye utilizando los mecanismos facilitados por la ACEDICOMMX principalmente a través del sitio Web <http://acedicom.edicomgroup.com/mx>.

7.2.3 Cambio de certificado de TSA

El certificado de la TSA puede ser cambiado en cualquier momento por otro certificado de TSA igualmente válido.

Este cambio no se comunicará a los usuarios del servicio, los cuales deberían confiar en todos los sellos emitidos por ACEDICOMMX y firmados con certificados válidos de TSA dentro de la jerarquía de certificación.

7.2.5. Destrucción de la clave privada de la TSA

La TSA garantiza, en base a sus sistemas de emisión y gestión de sellos de tiempo, que no se aceptarán peticiones que involucren a claves caducadas, y que se opera con las claves regeneradas en el instante que esta caducidad ocurre.

7.2.6. Gestión de los HSM

La TSA efectúa los análisis recomendados por los fabricantes de los HSM, acordes con la normalización técnica existente, para garantizar que los equipos no han sido manipulados y cumplen con los requisitos.

Los HSM se trasladan por personal interno de la TSA con roles autorizados para su inicialización y puesta en marcha en las dependencias internas seguras, con los controles de seguridad física adecuados, siendo desde este momento todas las manipulaciones registradas y auditadas.


En caso de cambio de HSM por cualquier motivo, las claves son borradas y destruidas, de acuerdo con los procedimientos que a tal fin suministra el fabricante.

La TSA gestiona los dispositivos de seguridad hardware de acuerdo al os estipulado en la CPS[1] de la ACEDICOMMX, procedimientos que son revisados de forma periódica por el auditor.

7.3 SELLADO DE TIEMPO

7.3.1. Token de sello de tiempo

Cada sello de tiempo emitido por la Autoridad de Sellado de Tiempo de la ACEDICOMMX incluye un identificador único de política, descrito en el capítulo

	PRÁCTICAS Y POLÍTICA DE SELLADO DE TIEMPO (TIMESTAMPING)	
	Edición 1.3	Página 18

5.2 “Identificación de la política de sellado de tiempo” de este documento. Los sellos de tiempo incluyen valores de fecha y hora identificables, mediante los cuales se puede llegar al valor de tiempo UTC.

La exactitud del tiempo usado en los sellos se describe en el capítulo 6.1.1 “Obligaciones de la TSA hacia sus subscriptores” de la presente política.

En caso de que sea imposible la obtención de la exactitud requerida por parte de la fuente de tiempos por cualquiera de los caminos establecidos, tal y como se describe en el capítulo 6.1.1, el token de sello de tiempo no será emitido.

Los tokens de sello de tiempo (TST) son emitidos conteniendo los datos recibidos en la petición (TSQ), garantizando así la presencia dato tiempo origen del servicio. Los sellos de tiempo son firmados por la clave privada de la Autoridad de Sellado de Tiempo, cuyo certificado asociado y extensiones se encuentran descritas en el capítulo 5.1 “Vista general” de la presente política. Estas claves y certificado han sido generados exclusivamente para este propósito por parte de la ACEDICOMMX.


La Autoridad de Sellado de Tiempo establece todo el procedimiento asociado a la generación de los tokens de sellos de tiempo utilizando el protocolo descrito en RFC-3161 [3].

7.3.2. Sincronización del reloj con UTC

Las fuentes de tiempos utilizadas, basadas en el protocolo NTP (Network Time Protocol) se auto calibran por distintos caminos, haciendo que la exactitud no disminuya por debajo de los requerimientos especificados (capítulo 5.1 del presente documento), utilizando **como referencia la del Centro Nacional de Metrología (CENAM)** y la sincronización GPS vía satélite. Se disponen de distintos caminos de sincronización de forma que la manipulación de los sistemas no afecta a la exactitud del sello de tiempo.

El Centro Nacional de Metrología (CENAM) mantiene en operación un conjunto de relojes atómicos con los cuales genera la escala de tiempo de menor incertidumbre en el país, denominada técnicamente Tiempo Universal Coordinado, y denotado por UTC(CNM). El UTC(CNM) es una realización física del UTC. De la escala de tiempo UTC(CNM) se generan los tiempos asociados a los tres husos horarios de la nación. El UTC(CNM) se mantiene con una incertidumbre por debajo de 100 milésimas de millonésima de segundo respecto a la escala de tiempo internacional denominada Tiempo Universal Coordinado, UTC.

A nivel interno la ACEDICOMMX dispone de mecanismos de seguridad que evitan la manipulación física de sus sistemas (información adicional en la CPS, apartado 5.1 “Controles de Seguridad Física”).

	PRÁCTICAS Y POLITICA DE SELLADO DE TIEMPO (TIMESTAMPING)	
	Edición 1.3	Página 19

La ACEDICOMMX incorpora mecanismos que detectan diferencias entre el tiempo suministrado y el que se incluye en los sellos de tiempo. El cálculo del tiempo se realiza de acuerdo al protocolo.

7.4 IMPLEMENTACIÓN DE LA SOLICITUD Y RESPUESTA DE SELLOS DE TIEMPO

Las solicitudes y respuestas de sellos se se adherirán a la sintaxis de la especificación “**RFC3161 Time Stamp Protocol (TSP)**” descrito en el Apartado 3.4. “Time-Stamp Protocol via http” de la especificación, con las restricciones de la norma ETSI TS 101 861.

La URL del servicio de Sellado de Tiempo de ACEDICOMMX es la especificada en el apartado 5.1 de este documento.

7.4.1. Protocolo Timestamp vía HTTP

Formato de la petición

Content-Type: application/timestamp-query

<<the ASN.1 DER-encoded Time-Stamp Request message>>

Formato de la respuesta

Content-Type: application/timestamp-reply

<<the ASN.1 DER-encoded Time-Stamp Response message>>

7.4.2 Formato de los mensajes

Existen dos tipos de mensajes: los que el cliente envía a la TSA, y los que envía la TSA al cliente. Todos los mensajes están representados en notación ASN.1

7.4.2.1 Timestamp Request

Este mensaje lo utiliza la entidad que quiere un sello de tiempo (solicitante) para acceder al servicio que ofrece una TSA. Tiene el siguiente formato:

```

TimeStampReq ::= SEQUENCE {
  version                INTEGER { v1(1) },
  messageImprint         MessageImprint,
  reqPolicy              TSAPolicyId                OPTIONAL,
  nonce                 INTEGER                    OPTIONAL,
  certReq               BOOLEAN                    DEFAULT FALSE,
  extensions             [0] IMPLICIT Extensions OPTIONAL
}

```

version	Versión de la petición TimeStamp (v1)
messageImprint	OID del algoritmo hash y el valor del hash de los datos
reqPolicy	OID de la política de la TSA Indica a la TSA la política bajo la cuál quiere que se proporcione el sello
Nonce	Si se incluye el nonce permite al cliente comprobar el retardo en la respuesta cuando no se dispone de reloj local. La respuesta debe contener este mismo número o se rechazará. El nonce es un número aleatorio con una elevada probabilidad de que el cliente lo genere una única vez (entero de 64 bits).
CertReq	Si el campo certReq está presente y con valor true, la clave publica de la TSA debe estar referenciada por el identificador ESSCertID dentro de un atributo SigningCertificate de la estructura SignedData en la respuesta. Ese campo además puede contener otros certificados. Si falta el campo certReq o tiene valor false entonces, el campo SigningCertificate de la estructura SignedData no debe aparecer en la respuesta.
extensions	Es una forma de permitir añadir nuevos campos en el futuro. Si se incluye algún campo de extensión que la TSA no reconozca, ésta devolverá un mensaje de error de extensión no aceptada (unacceptedExtension). Más información en: RFC 2459

```

MessageImprint ::= SEQUENCE {
    hashAlgorithm          AlgorithmIdentifier,
    hashedMessage          OCTET STRING
}

```

hashAlgorithm	OID del algoritmo hash: El algoritmo de hash indicado en <i>hashAlgorithm</i> debería ser uno conocido por la TSA. También comprobará que sea suficientemente fuerte. Si la TSA no reconoce el algoritmo usado o piensa que es débil, entonces la TSA denegará el servicio al cliente devolviendo un pkiStatusInfo de 'bad_alg'.
hashedMessage	Este campo contiene el hash de los datos que se quiere sellar. La longitud del hash tiene que coincidir con la longitud de hash del algoritmo utilizado

El mensaje **Timestamp Request** no identifica al cliente, y esta información no es validada por la TSA. En el caso en que la TSA requiera su identidad deberá utilizar un mecanismo alternativo de identificación o autenticación

7.4.2.2 Timestamp Response

Es la respuesta que la TSA da a una mensaje *time stamp request*. Tiene la siguiente representación:

```

TimeStampResp ::= SEQUENCE {

```

```

status          PKIStatusInfo,
timeStampToken  TimeStampToken  OPTIONAL
}

```

Status	Estado de la respuesta. Ver sección 3.2.3 del RFC 2510
timeStampToken	Este campo que contiene la marca de tiempo generado. Es una estructura ContentInfo que encapsula información firmada en una estructura TSTInfo . Está definida en la RFC 2630.

```

PKIStatusInfo ::= SEQUENCE {
    status          PKIStatus,
    statusString    PKIFreeText    OPTIONAL,
    failInfo        PKIFailureInfo OPTIONAL
}

```

Status	Estado de la respuesta: <ul style="list-style-type: none"> • granted(0): Marca de tiempo presente. • grantedWithMods(1): Marca de tiempo presente con modificaciones. • rejection(2): Petición rechazada • waiting(3): Esperando • revocationWarning(4) : Advertencia de revocación inminente • revocationNotification (5): Notificación de revocación
statusString	Puede usarse para indicar eventos de error
failInfo	Causas del fallo: <ul style="list-style-type: none"> • badAlg(0): Identificador de algoritmo no soportado • badRequest(2): Transacción no permitida o soportada • badDataFormat(5): Datos enviados con formato incorrecto • timeNotAvailable(14): Origen de tiempo no disponible • unacceptedPolicy(15): Política solicitada no soportada • unacceptedExtension(16): Extensión no soportada • addInfoNotAvailable(17): Información adicional no disponible • systemFailure(25): Error del sistema

```

TSTInfo ::= SEQUENCE {
    version          INTEGER { v1(1) },
    policy           TSAPolicyId,
    messageImprint   MessageImprint,
    serialNumber     INTEGER,
    genTime          GeneralizedTime,
    accuracy         Accuracy          OPTIONAL,
    ordering         BOOLEAN           DEFAULT FALSE,
    nonce            INTEGER           OPTIONAL,
    tsa              [0] GeneralName   OPTIONAL,
    extensions       [1] IMPLICIT Extensions OPTIONAL
}

```


Version	Versión de la respuesta TimeStamp (v1)
ReqPolicy	OID de la política de la TSA Indica la política de la TSA bajo la cual se proporciona el sello, si se ha

	generado el sello, será igual al del mensaje de petición
messageImprint	OID del algoritmo hash y el valor del hash de los datos. Debe tener el mismo valor que el campo correspondiente de la petición.
SerialNumber	Es un entero asignado por la TSA y debe ser único para cada sello que genere. Por tanto, un sello será identificado por el nombre de la TSA que lo generó y el número de serie asignado. Permite hasta 160 bits
genTime	<p>Es el instante de tiempo en el que se creó el sello. Tanto ISO como el IETF expresan el instante de tiempo referido a la escala <i>UTC</i>, para evitar confusiones con las horas locales. El formato debe ser el siguiente:</p> <p>CC YY MM DD hh mm ss Z</p> <ul style="list-style-type: none"> • CC representa el siglo (19-99) • YY representa el año (00-99) • MM representa el mes (01-12) • DD representa el día (01-31) • hh representa la hora (00-23) • mm representa los minutos (00-59) • ss representa los segundos (00-59) • Z viene de <i>zulu</i>, que es como se conoce a la escala <i>UTC</i>
accuracy	<p>Representa la desviación del tiempo UTC contenido en <i>genTime</i>, en los casos que sea necesario, proporciona una precisión incluso de microsegundos:</p> <pre>Accuracy ::= SEQUENCE { seconds [1] Integer OPTIONAL, millis [2] Integer (1..999) OPTIONAL, micros [3] Integer (1..999) OPTIONAL, }</pre> <p>Cuando este campo no está presente la precisión puede obtener a través de otros métodos, por ejemplo TSAPolicyId.</p>
ordering	<p>Si falta el campo <i>ordering</i> o está presente y tiene valor <i>false</i>, entonces el campo genTime solo indica el momento en el que la marca de tiempo ha sido creada por la TSA.</p> <p>En este caso, el orden de las marcas de tiempo emitidas por una misma TSA o distintas TSAs solo es posible cuando la diferencia entre el <i>genTime</i> de la primera marca de tiempo es mayor que la suma de las precisiones del <i>genTime</i> de cada marca de tiempo.</p>
nonce	El nonce es un número aleatorio con una elevada probabilidad de que el cliente lo genere una única vez (entero de 64 bits). Debe tener el mismo valor que el campo correspondiente de la petición.
Tsa	Identificador de la TSA
extensions	Es una forma de permitir añadir nuevos campos en el futuro. Más información en: RFC 2459

7.4.2.3 Validate Request

Es el mensaje que una entidad envía a una TSA cuando quiere comprobar la validez y la autenticidad de un sello. En la RFC 3161 del IETF no se contempla el proceso de verificación del sello de tiempo:

```
ValidateRequest ::= SEQUENCE {
    version      INTEGER { v1(0) },
    tst          TimeStampToken,
    requestID    [0] OCTET STRING OPTIONAL
}
```

	PRÁCTICAS Y POLÍTICA DE SELLADO DE TIEMPO (TIMESTAMPING)	
	Edición 1.3	Página 23

- *tst*: contiene el sello que se quiere verificar
- *requestID*: identificador que se utiliza para vincular una petición con su respuesta

7.4.2.4 Validate Reply

La TSA envía este mensaje como respuesta a una petición de verificación:

```

ValidateReply ::= SEQUENCE {
    version      INTEGER { v1(0) },
    status       PKIStatusInfo,
    tst          TimeStampToken,
    requestID    [0] OCTET STRING OPTIONAL
}

```

7.5. OPERACIÓN Y GESTIÓN DE LA TSA

7.5.1. Gestión de la seguridad

Todos los elementos relativos al control de la seguridad se describen en la Política de Seguridad de la Información de la ACEDICOMMX de Sellado de Tiempo y en la CPS [1], capítulo 5.2 “Controles procedimentales”, siendo acordes a lo establecido en ISO-17799.

7.5.2. Control de riesgos e inventario de activos


Todos los elementos relativos al control de riesgos e inventario de activos se encuentran en documentación de la ACEDICOMMX clasificada de USO INTERNO, revisada de forma periódica por el auditor. Se sigue lo establecido en la especificación ISO-17799.

La ACEDICOMMX realizará pruebas periódicas de su Plan de continuidad y actualizará con ello el análisis de riesgos.

7.5.3. Seguridad del personal

Características del personal, así como los roles establecidos e incompatibilidades, se describen en la CPS[1], capítulo 5.3 “Controles de seguridad de personal” y en el documento de gestión de personal clasificados de uso interno, solo se proporciona a quien acredite necesidad de conocerla y son revisados de forma periódica por el auditor. Se sigue lo establecido en la especificación ISO-17799.

7.5.4. Seguridad física

	PRÁCTICAS Y POLITICA DE SELLADO DE TIEMPO (TIMESTAMPING)	
	Edición 1.3	Página 24

La descripción de la seguridad física se detalla en la Política de Seguridad de la Información de la ACEDICOMMX y en la CPS[1], capítulo 5 “Controles de seguridad física, procedural y de personal”. Estos controles cumplen con los requerimientos normativos del documento ISO-17799.

7.5.5. Gestión de las operaciones

La Autoridad de Sellado de Tiempo de la ACEDICOMMX tiene establecidos controles de seguridad procedimental que afectan a todas las operaciones que involucran la emisión y el control de sellos de tiempo, así como en el manejo y control de los sistemas, sistemas de control de incidencias y gestión de copias de seguridad. La parte publica de esta información se encuentra la CPS [1], el resto se ha clasificado de uso interno.

7.5.6. Gestión de acceso a los sistemas

Los sistemas responsables de la emisión y control de los sellos de tiempo se encuentran en las dependencias de la ACEDICOMMX, compartiendo las medidas de seguridad física de su entorno de confianza. En concreto, el recinto se encuentra protegido por un sistema de alarma contra intrusiones, operadas 24X7 por personal autorizado.

El acceso lógico a los sistemas esta limitado a personal autorizado.

7.5.7. Mantenimiento y despliegue de sistemas de confianza


Dentro de la operación de la Autoridad de Sellado de Tiempo, la generación de las claves de la TSA siempre se lleva a cabo dentro del entorno de confianza de la ACEDICOMMX, por personal interno con roles autorizados, como se describe en el capítulo 7.2.1 “Generación de claves de la TSA” de la presente política.

Todas las modificaciones que afectan al servicio de sellado de tiempo involucran, aparte de los análisis funcionales y de requerimientos, un análisis de seguridad y una gestión del cambio controlada.

7.5.8. Compromiso de los servicios de sellado de tiempo.

En caso de compromiso de los servicios de sellado de tiempo, se harán efectivos los procedimientos descritos en el Plan de Continuidad de Servicio de la TSA de la ACEDICOMMX.

Si este compromiso afecta la claves privadas de la Autoridad de Sellado o a la pérdida de exactitud de los sellos de tiempo, la información relevante será comunicada a los suscriptores del servicio y a partes confiantes, y se interrumpirá el servicio.

	PRÁCTICAS Y POLITICA DE SELLADO DE TIEMPO (TIMESTAMPING)	
	Edición 1.3	Página 25

La información suministrada incluirá la naturaleza del compromiso, y las herramientas o sistemas necesarios para la comprobación de sus sellos de tiempo, garantizando la identificación de los elementos comprometidos.

7.5.9 Cese de la actividad de la TSA

La Autoridad de Sellado de Tiempo garantiza la minimización del impacto en caso de cese del servicio de sellado de tiempo. En particular, asegura la continuidad de la información requerida para verificar la corrección de los sellos de tiempo.

Antes del cese de su actividad la TSA realizará las siguientes actuaciones:

- Informará a todos los suscriptores, usuarios o entidades con los cuales tenga acuerdos u otro tipo de relación del cese con la anticipación mínima de 2 meses, o el periodo que establezca la legislación vigente.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la TSA en el procedimiento de emisión de sellos de tiempo.
- Informará a la administración competente, con la antelación indicada, el cese de su actividad y el destino que se vaya a dar a los sellos de tiempo emitidos hasta la fecha, especificando, en su caso, si se va a transferir la gestión y a quien.

7.5.10. Cumplimiento de los requisitos legales


La TSA de la ACEDICOMMX, como Autoridad de Sellado de Tiempo, actúa acorde a los requisitos establecidos por la legislación mexicana vigente, en lo que hace referencia a la protección de datos y a la gestión y operación de servicios y sistemas informáticos, siguiendo en los casos en que no hay ley aplicable, las directrices técnicas establecidas por los organismos cualificados (ETSI, CEN, etc).

7.5.11. Registro de información relativa a la operación del servicio de sellado de tiempo

La ACEDICOMMX, como Autoridad de Sellado de Tiempo, incorpora mecanismos para la creación y control de registros de los eventos derivados de su operación. Estos mecanismos se encuentran descritos en la CPS[1], capítulo 4.5 “Procedimientos de control de seguridad”.

7.5.12 Esquema organizativo

La Autoridad de Sellado de Tiempo se encuentra incluido dentro de la Autoridad de Certificación de EDICOM, siendo uno de sus servicios adicionales. Los datos del esquema organizativo se encuentran en la CPS [1], capítulo 1.4, “Datos de Contacto”.

	PRÁCTICAS Y POLÍTICA DE SELLADO DE TIEMPO (TIMESTAMPING)	
	Edición 1.3	Página 26

8 PROTECCIÓN DE DATOS PERSONALES

La TSA de ACEDICOMMX dispone de una Política de Privacidad, publicada en la web de ACEDICOMMX, mediante la que se informa sobre la política de protección de datos de carácter personal de la ACEDICOMMX.

8.1. Plan de Protección de Datos Personales.

La TSA de ACEDICOMMX desarrolla una política de privacidad, de acuerdo con el Código de Comercio y las Reglas Generales para los PSC de 10 de agosto de 2004, de Protección de Datos de Carácter Personal.

8.2. Procedimientos de protección de confidencialidad de la información.

También se han tomado medidas especiales de seguridad para proteger la información privada de los solicitantes de Sellos Digitales de tiempo durante el registro tales como:

- Carta de confidencialidad de los agentes registradores por la que se obligan y comprometen a guardar confidencialidad de los datos que manipulan en virtud de su puesto de trabajo.
- Políticas y procedimientos de clasificación de la información que clasifican la información recogida como confidencial y por lo tanto sujeta a las medidas internas de protección de datos personales
- En el sistema de registro se utilizan políticas de contraseñas robustas
- Los datos digitalizados se almacenan en servidores y directorios especialmente protegidos mediante permisos concedidos exclusivamente por el equipo administrador
- Los datos en papel se almacenan en archiveros seguros cerrados.

8.3. Información considerada privada.


Se consideran datos de carácter personal cualquier información relativa a personas físicas identificadas o identificables.

Toda la información personal que no haya de ser incluida en los sellos de tiempo se considera información personal de carácter privado.

En cualquier caso, los siguientes datos son considerados como información privada:

- Solicitudes de registro en servicio de emisión de sellos de tiempo, aprobadas o denegadas, así como toda otra información personal obtenida para la puesta en marcha del servicio al usuario.
- Toda otra información identificada como "Información privada"

Está protegida frente a su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado.

	PRÁCTICAS Y POLITICA DE SELLADO DE TIEMPO (TIMESTAMPING)	
	Edición 1.3	Página 27

8.4. Información no considerada privada.

Esta información hace referencia a la información personal que se pueda incluir en los sellos de tiempo.

En todo caso, es considerada no confidencial la siguiente información:

- El nombre y los apellidos del suscriptor del servicio.
- La dirección electrónica del suscriptor del servicio.
- La información contenida en el depósito de sellos de tiempo de la TSA.

8.5. Responsabilidades.

La TSA de la ACEDICOMMX garantiza el cumplimiento de sus obligaciones legales como prestador de servicios de emisión de sellos digitales de tiempo, y en virtud de esto, responderá por los daños y perjuicios que cause en el ejercicio de la actividad por el incumplimiento de las prescripciones legales relativas a la protección de datos personales.

La TSA de la ACEDICOMMX incluye en el documento “Política de Privacidad” publicado en la web de la ACEDICOMMX su procedimiento de notificación, gestión y respuesta ante las incidencias relacionadas con los datos personales. Este procedimiento contiene un registro en el que se hace constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, la persona a quien se comunica la notificación y los efectos que se derivan.

8.6. Prestación del consentimiento en el uso de los datos personales.

Para la prestación del servicio, la TSA de la ACEDICOMMX habrá de obtener el consentimiento de los titulares de los datos necesarios para prestación los servicios de emisión de sellos digitales. Se entenderá obtenido el consentimiento con la firma del contrato por parte del usuario.

8.7. Comunicación de la información a autoridades administrativas y/o judiciales.


La TSA de la ACEDICOMMX sólo podrá comunicar informaciones calificadas como confidencial o que contengan datos de carácter personal en aquellos supuestos en los que así se le requiera por la autoridad pública competente y en los supuestos previstos legalmente.

En concreto, la TSA de la ACEDICOMMX está obligada a revelar la identidad de los firmantes cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tengan atribuidas.

9. RESOLUCIÓN DE CONFLICTOS.

9.1. Resolución extrajudicial de conflictos.

La TSA de la ACEDICOMMX establecerá en el contrato de servicios de Sellado Digital de Tiempo con los suscriptores, los procedimientos de

	PRÁCTICAS Y POLÍTICA DE SELLADO DE TIEMPO (TIMESTAMPING)	
	Edición 1.3	Página 28

mediación, arbitraje y resolución de conflictos que se consideren oportunos, todo ello sin perjuicio de las vías y acciones legales correspondientes.

9.2. Jurisdicción competente.

La TSA de la ACEDICOMMX establece en el contrato de servicios de Sellado Digital de Tiempo con sus suscriptores, los tribunales federales competentes en el Distrito Federal, con renuncia a la jurisdicción que les corresponda o pueda corresponderles en virtud de su domicilio presente o futuro.

10. LEGISLACIÓN APLICABLE

El funcionamiento y operaciones de la TSA de ACEDICOMMX, así como la presente política están regidos por la legislación federal vigente.

Explícitamente se asumen como de aplicación las siguientes normas:

REFORMAS AL CODIGO DE COMERCIO

- Reformas al Código de Comercio en materia de firma electrónica publicadas el 29 de agosto del 2003 en el D.O.F.
- Reformas al Código de Comercio en materia de firma electrónica publicadas el 29 de mayo del 2000 en el D.O.F.

NORMAS OFICIALES

- NORMA Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales- Requisitos que deben observarse para la conservación de mensajes de datos publicada el 4 de junio del 2002 en el D.O.F.

REGLAMENTOS Y REGLAS

- Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación (Publicado el 19 de julio del 2004 en el D.O.F.)
- Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación (Publicadas el 10 de agosto del 2004 en el D.O.F.)
- ACUERDO que modifica las Reglas Generales a las que deberán sujetarse los prestadores de servicios de certificación (Publicado el 5 de marzo del 2007 en el D.O.F.)