Certificamos Información Digital

POLÍTICA DE CERTIFICADOS SELLADO DE TIEMPO (PC-TSA)	
SGSI - GG	Código: **PCTSA-DES-DC-00021**
	Versión: 1.0
	Clasificación de Información: Documento de Acceso Público

POLÍTICA DE CERTIFICADOS PARA SELLADO DE TIEMPO (PC-TSA)

Aprobado por:	**Firma de Aprobación:**
Galo Santiago Becerra Gordón Gerente General	 Digitally signed by GALO SANTIAGO BECERRA GORDÓN
	Fecha de Aprobación: 05 de febrero de 2026

Tabla de Contenidos / Índice

1. Presentación

DICERT DISTRIBUIDORA INTERNACIONAL DE CERTIFICACION ELECTRONICA S.A. es una compañía legalmente constituida bajo las leyes ecuatorianas, con domicilio principal en la ciudad de Quito, dedicada a la provisión de servicios de confianza electrónica, incluyendo la emisión de certificados de firma electrónica y servicios de sellado de tiempo.

2. Introducción

La presente Política de Certificados para Sellado de Tiempo (PC-TSA) constituye el conjunto de reglas que definen la aplicabilidad de los certificados emitidos por DICERT para su Autoridad de Sellado de Tiempo (Time Stamping Authority - TSA). El documento ha sido redactado siguiendo estrictamente las directrices del estándar RFC 3647 y la normativa técnica ecuatoriana vigente. La PC-TSA detalla los requisitos técnicos, operativos y legales que garantizan la integridad cronológica de los mensajes de datos procesados por la infraestructura de DICERT, asegurando el no repudio del momento de creación o firma de un documento electrónico.

2.1. Visión General

La Infraestructura de Clave Pública (PKI) de DICERT integra el servicio de sellado de tiempo como un componente crítico para la seguridad de las transacciones digitales. El sellado de tiempo permite certificar que un conjunto de datos existía en un instante temporal específico, vinculando de manera indisoluble el hash de la información con la hora oficial proporcionada por fuentes de tiempo confiables y auditadas. Este servicio es fundamental para procesos de desmaterialización, facturación electrónica y firma electrónica de largo plazo (AdES-T/LT/LTA), cumpliendo con los requisitos de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su reglamento y la Norma Técnica ARCOTEL-2024-0176.

2.2. Nombre e Identificación del Documento

El presente documento se denomina 'Política de Certificados para Sellado de Tiempo DICERT (PC-TSA)'. Para su identificación inequívoca en sistemas informáticos y aplicaciones PKI, se le asigna el siguiente Identificador de Objeto (Object Identifier - OID):

Documento	**Identificador de Objeto (OID)**
Política de Certificados para Sellado de Tiempo (PC-TSA)	1.3.6.1.4.1.62486.2.5.1

Declaración de Prácticas de Certificación (DPC) DICERT	1.3.6.1.4.1.62486.1

El uso de este OID en el campo certificatePolicies del certificado de la TSA asegura que las partes confiantes puedan identificar la normativa bajo la cual se emiten los sellos de tiempo.

2.3. Participantes de la PKI

2.3.1. Autoridad de Certificación Raíz (AC Raíz)

La AC Raíz de DICERT es la autoridad de confianza máxima que emite certificados para las AC Subordinadas (Intermedias). La AC Raíz mantiene sus claves privadas en un entorno 'offline' de alta seguridad.

2.3.2. Autoridad de Registro (AR)

En el contexto de la PC-TSA, la AR es responsable de verificar la identidad y los permisos de las entidades o componentes que solicitan el servicio de sellado de tiempo, asegurando que la emisión del certificado de infraestructura TSA cumpla con los estándares de DICERT.

2.3.3. Suscriptores (Titulares)

Para el sellado de tiempo, el suscriptor es habitualmente un componente lógico o servidor operado por la propia ECI o por un Tercero Vinculado autorizado para proveer el servicio de estampado cronológico.

2.3.4. Partes Confiables

Cualquier persona natural o jurídica que recibe un mensaje de datos sellado cronológicamente y confía en la exactitud de la marca de tiempo basándose en la acreditación de DICERT ante ARCOTEL.

2.3.5. Otros Participantes

Incluye proveedores de infraestructura tecnológica (como Amazon Web Services), auditores externos y entidades de control gubernamental.

2.4. Uso de los Certificados

2.4.1. Usos Permitidos

Los certificados de sellado de tiempo emitidos bajo esta política están restringidos exclusivamente a la firma de tokens de sello de tiempo (Time Stamp Tokens - TST) conforme al protocolo RFC 3161. Son adecuados para:

- Garantizar la existencia de documentos electrónicos antes de una fecha determinada.

- Soportar firmas electrónicas avanzadas longevas.
- Registros de auditoría inmutables en sistemas judiciales o bancarios.

2.4.2. Usos Prohibidos

No se permite el uso de estos certificados para:

- Firma de mensajes de correo electrónico personales.
- Cifrado de archivos.
- Autenticación de clientes en redes privadas virtuales (VPN).

2.5. Administración de la Política

2.5.1 Organización que administra el documento

La responsabilidad de la gestión, revisión y actualización de esta PC-TSA recae exclusivamente en la Gerencia General de DICERT.

2.5.2 Persona de contacto

Cualquier consulta técnica o legal relacionada con este documento debe dirigirse a:

- **Atención:** Soporte Técnico.
- **Correo electrónico:** soporte@dicert.com.ec

2.5.3 Persona que determina la idoneidad de la DPC para la política

La Gerencia General de DICERT actúa como el órgano competente para declarar que las prácticas operativas descritas en la DPC son suficientes para soportar las exigencias de esta Política de Certificados.

2.5.4 Procedimientos de aprobación del CPS

La aprobación del presente documento requiere un informe técnico de cumplimiento y la rúbrica formal del Gerente General. Toda versión aprobada debe ser notificada a ARCOTEL en el plazo de 15 días tras su emisión.

2.6. Definiciones y Acrónimos

- **TSA:** Autoridad de Sellado de Tiempo (Time Stamping Authority).
- **TST:** Token de Sello de Tiempo (Time Stamp Token).
- **UTC:** Tiempo Universal Coordinado.
- **NTP:** Protocolo de Tiempo de Red.

3. Publicación y Responsabilidades del Repositorio

3.1. Repositorios

DICERT opera un repositorio digital de acceso público permanente (24/7) que aloja la documentación normativa de su PKI. La infraestructura del repositorio se basa en servicios de nube de alta disponibilidad con redundancia geográfica.

3.2. Publicación de Información de Certificación

En el repositorio se publican:

- La Declaración de Prácticas de Certificación (DPC).
- La Política de Certificados para Sellado de Tiempo (PC-TSA).
- El Certificado de la TSA y las cadenas de confianza.
- Las Listas de Certificados Revocados (CRL).

3.3. Tiempo o Frecuencia de Publicación

DICERT garantiza que las CRLs se generen y publiquen al menos cada 24 horas. La información sobre el estado de los certificados mediante el protocolo OCSP está disponible en tiempo real inmediatamente después de cualquier cambio de estatus.

3.4. Control de acceso a los repositorios

El acceso para consulta es irrestricto y gratuito. La modificación del contenido del repositorio está protegida mediante controles de acceso basados en roles (RBAC) y autenticación multifactor (MFA), auditados periódicamente.

4. Identificación y Autenticación

4.1. Nombres

Los certificados de sellado de tiempo utilizan Nombres Distinguidos (DN) conforme al estándar X.501 y la codificación ETSI EN 319 412-1.

4.1.1 Tipos de Nombres

Los atributos que conforman el campo 'Subject' del certificado TSA incluyen:

Atributo	Valor Requerido

Country Name (C)	EC
Locality Name (L)	Ciudad de operación (p.ej. QUITO)
Organization Name (O)	DICERT DISTRIBUIDORA INTERNACIONAL...
Organizational Unit (OU)	UNIDAD DE SELLADO DE TIEMPO
Common Name (CN)	TSA DICERT 01 (o identificador secuencial)
Serial Number	RUC de la entidad (VAT-EC-XXXXXXXXXXXXX).

4.2. Validación de Identidad Inicial

4.2.1. Método para probar la posesión de la clave privada

La entidad solicitante debe enviar una Solicitud de Firma de Certificado (CSR) generada dentro de un dispositivo criptográfico seguro (HSM). La AC verifica la firma del CSR para confirmar que el solicitante posee la clave privada asociada.

4.2.2. Autenticación de la Identidad de la organización

DICERT verifica su propia existencia legal y vigencia de su acreditación ante ARCOTEL mediante la consulta de los registros públicos y la resolución de acreditación correspondiente.

5. Requisitos Operativos del Ciclo de Vida del Certificado

5.1. Solicitud de Certificado

La solicitud del certificado para el servicio TSA es un proceso interno controlado. Debe ser iniciada por el Oficial de Seguridad de la Información y aprobada por la Gerencia General.

5.2. Procesamiento de Solicitudes de Certificado

Se realiza una verificación técnica de que los parámetros de la clave (RSA 2048 o superior) y el algoritmo de firma (SHA-256) cumplen con la normativa ARCOTEL-2024-0176.

5.3. Emisión de Certificado

La AC Intermedia de DICERT firma electrónicamente el certificado de la TSA, integrando el OID de la

política y las extensiones de uso de clave específicas para sellado de tiempo.[2]

5.4. Revocación y Suspensión de Certificados

5.4.1. Circunstancias para la Revocación

El certificado de la TSA será revocado inmediatamente si:

- Existe sospecha razonable de compromiso de la clave privada.
- Se detecta una deriva de tiempo superior a 1 segundo respecto a UTC que no puede corregirse.
- Cesa la acreditación del servicio ante el organismo de control.

5.5. Servicios de Estatus de Certificados

DICERT proporciona validación mediante OCSP (Online Certificate Status Protocol) y CRL, permitiendo a las aplicaciones verificar la vigencia de la marca de tiempo de forma ágil.

6. Controles Gestión, Operativos y Físicos

6.1. Controles de Seguridad Física

La infraestructura crítica de DICERT se aloja en centros de datos que cumplen con estándares internacionales de seguridad física, incluyendo control de acceso biométrico, vigilancia 24/7 y sistemas contra incendios automáticos.

6.2. Controles de Procedimientos

Se implementa la regla de 'control mutuo' para tareas sensibles. La activación de la clave privada de la AC o de la TSA requiere la concurrencia de al menos dos personas en roles de confianza autorizados.

6.3. Controles de Seguridad del Personal

Todo el personal involucrado en la operación de la TSA debe someterse a verificaciones de antecedentes y firmar acuerdos de confidencialidad. Reciben capacitación continua en criptografía y gestión de riesgos.

6.4. Procedimientos de Registro de Auditorías

DICERT registra todos los eventos del sistema TSA, incluyendo inicios de sesión, cambios de configuración, sincronizaciones de tiempo y generación de sellos. Estos registros se archivan de forma segura por un periodo mínimo de 10 años.

7. Controles Técnicos de Seguridad

7.1. Generación de par de Llaves e Instalación

Las claves de la TSA se generan exclusivamente dentro de Módulos de Seguridad de Hardware (HSM) certificados FIPS 140-2 Nivel 3 o superior.

7.1.5. Tamaños de Claves

Se utilizan longitudes de clave RSA de al menos 2048 bits para la TSA, asegurando resistencia criptográfica frente a ataques contemporáneos.

7.2. Sellado de Tiempo (Protocolos y Sincronización)

De conformidad con los Artículos 21 al 28 de la Resolución ARCOTEL-2024-0176, el servicio de sellado de tiempo de DICERT cumple con:

- **Margen de Error:** Máximo de un (1) segundo respecto a la hora UTC oficial.
- **Fuentes de Tiempo:** Sincronización mediante GPS y protocolo NTP redundante.
- **Auditabilidad:** Registro inmutable de cada transacción de sellado, accesible para auditorías estatales.[1]

8. Perfiles de Certificados, CRL y OCSP

8.1. Perfil del Certificado

El certificado de la TSA de DICERT se ajusta al perfil técnico definido en el Anexo 5 de la norma ARCOTEL.

8.1.1. Extensiones de los certificados (Anexo 5 de la Norma Técnica ARCOTEL-2024-0176)

Extensión	**Valor / Criticidad**
Authority Key Identifier	Identificador de la AC emisora
Subject Key Identifier	Identificador de la clave TSA
Key Usage	Digital Signature (Crítica)
Extended Key Usage	Time Stamping (1.3.6.1.5.5.7.3.8) (Crítica)

Certificate Policies	1.3.6.1.4.1.62486.2.5.1 (No Crítica)
Authority Info Access	Acceso al OCSP y certificado del emisor
Basic Constraints	Subject Type: End Entity (Crítica).

9. Auditorías de Cumplimiento y Otras Evaluaciones

9.1. Frecuencia y Circunstancia de la evaluación

DICERT se somete anualmente a una auditoría externa de seguridad informática y cumplimiento PKI realizada por firmas independientes calificadas por ARCOTEL.

10. Otros Asuntos Comerciales y Legales

10.1. Tarifas

DICERT publica en su portal web las tarifas vigentes por la emisión de sellos de tiempo, basadas generalmente en planes de volumen de transacciones.

10.2. Representaciones y Garantías

10.2.1. Representaciones y Garantías de la AC

DICERT garantiza que su TSA opera con una precisión temporal certificada y que las claves privadas están protegidas por hardware de grado militar. Se compromete al cumplimiento total de la Ley de Comercio Electrónico y Normas Técnicas de ARCOTEL.

10.3. Limitación de Responsabilidad

La responsabilidad financiera de DICERT frente a fallos técnicos en el sellado de tiempo se limita, en el marco legal, hasta el valor abonado por el suscriptor por dicho servicio, salvo pacto en contrario o negligencia grave debidamente probada.

10.4. Ley Aplicable

La presente política se rige por las leyes de la República del Ecuador, sometiéndose las controversias no resueltas amigablemente al Centro de Arbitraje y Mediación de la Cámara de Comercio de Quito.

11. Control de Cambios

POLÍTICAS DE CERTIFICADOS PARA SELLADOS DE TIEMPO DICERT						
CÓDIGO: PCTSA-DES-DC-00021					**CLASIFICACIÓN:** Documento de Acceso Público	
VERSIÓN	**DETALLE**	**ELABORADO POR:**	**FECHA APRUEBA**	**REVISADO POR:**	**FECHA PUBLICACIÓN**	**LOCALIZACIÓN**
1.0	Versión Inicial	Paúl Quiñonez	08/04/2025	Galo Becerra	04/04/2025	https://dicert.com.ec/links

12. Firmas de Responsabilidad

Elaborado por:	**Firma**
Nombre: Paúl Quiñonez	Paul Sebastian Quiñonez Salas Firmado digitalmente por Paul Sebastian Quiñonez Salas Fecha: 2026.03.02 15:13:26 -05'00'

Aprobado por:	**Firma**
Nombre: Galo Becerra Cargo: Gerente General	Digitally signed by GALO SANTIAGO BECERRA GORDÓN