POLÍTICAS DE CERTIFICADOS DE VALIDACIÓN OCSP

Código	Nombre	Versión	Clasificación de la información
POP-PL-114	**Políticas de Certificados de Validación OCSP**	1	Pública

Título del Documento	**Políticas de Certificados de Validación OCSP**
Versión	1
Grupo de Trabajo	Comité de Gerencia
Estado del documento	Final
Fecha de emisión	17/02/2025
Fecha de inicio de vigencia	17/02/2025
OID (Object Identifier)	1.3.6.1.4.1.62566.2.6.1
Ubicación de la Política	https://letmi.app/documentos/Marco_regulatorio/politicas/Politicas_de_Certificados_de_validación_OCSP_V1.pdf
Elaboró	Coordinador de Operaciones
Revisó	Sistema Integrado de Gestión
Aprobó	Apoderado

Control de Cambios

Versión	Fecha	Cambio/Modificación
1	17/02/2025	Documento inicial conforme al desarrollo del plan de acción de ARCOTEL

CONTENIDO

1. INTRODUCCIÓN

El presente documento especifica las Políticas de Certificados de Validación OCSP (en adelante PC) para los diferentes certificados emitidos por la ECI Letmi Ecuador S.A.

El objeto de la PC es definir aquellos requerimientos que son necesarios para el funcionamiento de los Servicios de Validación de certificados emitidos por ECI Letmi Ecuador S.A.

En la medida en que en la DPC de la ECI Letmi Ecuador S.A se establece todos los requerimientos genéricos acerca de sistema de seguridad, soporte, administración y emisión de los Certificados ECI Letmi Ecuador S.A, las políticas harán referencia únicamente los requerimientos específicos de validación remitiéndose en el resto de los términos a lo establecido en la DPC.
De esta forma, los distintos certificados de la ECI Letmi Ecuador S.A, deberán ajustarse a los requerimientos genéricos y niveles de seguridad que se detallan en la DPC y a los requerimientos específicos para cada uno definidos en este documento.

ECI Letmi Ecuador S.A deberá informar a los titular de la firma y/o Responsables de la existencia de este documento donde se da respuesta a las PC de los distintos certificados emitidos por ECI Letmi Ecuador S.A.

1.1 RESUMEN

Políticas de Certificados de Validación OCSP , en adelante **Política** es un documento elaborado por **Letmi Ecuador S.A (en adelante Letmi Ecuador S.A)** que, actuando como una Entidad de Certificación de Información, contiene las normas, procedimientos que la **Entidad de Certificación de Información (en adelante Letmi Ecuador S.A)** como **Prestador de Servicios de Certificación digital (PSC)** aplica como lineamiento para prestar el Servicio de acuerdo con los reglamentos definidos en el territorio de Ecuador

Este documento aplica para los productos y servicios acreditados por Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL.

DATOS DE LA ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN:

Razón Social:	**Letmi Ecuador S.A**
Sigla:	**Letmi Ecuador S.A**
Número de RUC:	1793221101001
Registro Mercantil No: **Certificado de Existencia y Representante Legal:**	42253
Estado del registro mercantil:	Activo
Dirección social y correspondencia:	Calle Corea #126 Av Amazonas Edificio Belmonte Oficina 5 Piso 5 / Barrio Iñaquito
Ciudad / País:	Quito - Ecuador
Teléfono:	+59 (3) 02 2435200 (principal) +59 (3) 02 2921948 (alterno)
Correo electrónico:	info@letmi.app
Página Web:	https://letmi.app/

1.2. Nombre e identificación del documento

1.2.1. Criterio de Identificación de las Políticas (OID)

La forma de identificar los distintos tipos de certificados digitales de ECI Letmi Ecuador S.A es a través de identificadores de objeto (OID's). Un OID concreto permite a las aplicaciones distinguir claramente el certificado que se presenta.

El identificador de la PC está compuesto por una serie de números separados entre sí por puntos y con un significado concreto de cada uno de ellos.

Partiendo del OID, se distingue el certificado genérico ECI Letmi Ecuador S.A, y su vez, partiendo de este certificado de ECI Letmi Ecuador S.A se definen diferentes subtipos en función a algunas características específicas, como son:

1.2.2. OID de las Políticas

El siguiente cuadro muestra los diferentes certificados emitidos por la ECI Letmi Ecuador S.A, y los OID de sus correspondiente PC, en función de las distintas variables definidas en el anterior apartado:

OID	**DESCRIPCIÓN**
1.3.6.1.4.1.62566.2.6.1	Política de Certificados de Validación OCSP

CERTIFICADO DE VALIDACIÓN OCSP					
Campo	**Descripción**	**Obligatorio**	**Crítico**	**Observaciones**	**OID**
1. Basic structure	Estructura básica del certificado	Sí			
1.1. Version	"2"	Sí		El literal "2" corresponde a la versión 3. X.509 v3	
1.2. Serial Number	Establecido automáticamente por la AC. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.	
1.3. Signature Algorithm	1.2.840.113549.1.1.11	Sí			
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11	
1.3.2. Parameters	No aplicable	No			
1.4. Issuer		Sí			
1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)	Sí			2.5.4.6
1.4.2. Locality Name (L)	Localidad de la AC Subordinada (Ciudad) Ej. "QUITO"	Sí			2.5.4.7
1.4.3. Organizational Unit (OU)	Nombre de la Unidad Organizativa de la AC Subordinada Ej. "CA RSA SUB (Certification Services)"	No			2.5.4.11
1.4.4. Organization Name (O)	Nombre de la organización de la AC Subordinada Ej."LETMI ECUADOR S.A."	Sí			2.5.4.10
1.4.5. Common Name (CN)	Nombre de la AC Subordinada Ej."LETMI RSA SUB C1"	Sí			2.5.4.3
1.4.6. Organization Identifier	Identificador de la AC Subordinada "VAT(CÓDIGO_PAÍS)-IDENTIFICADOR_ORGANIZACIÓN" Ej. "VATEC-1793221101001"	No		Codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio	2.5.4.97
1.5. Validity	Se recomienda máximo 5 años (uso actual 2 años)	Sí			
1.5.1. Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ	
1.5.2. Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ	
1.6. Subject		Sí			
1.6.1. Country Name (C)	Código del País "EC" (ISO 3166)	Sí			2.5.4.6
1.6.2. Locality Name (L)	Localidad de la AC Subordinada (Ciudad) Ej. QUITO	Sí			2.5.4.7
1.6.3. Organizational Unit Name (OU)	Nombre de la Unidad Organizativa de la AC Subordinada Ej. "CA RSA SUB (OCSP Responder)"	Sí			2.5.4.11
1.6.4. Organization Name (O)	Organización de la AC Subordinada Ej."LETMI ECUADOR S.A."	Sí			2.5.4.10
1.6.5. Common Name (CN)	Nombre de la AC Subordinada Ej."LETMI RSA SUB C1"	Sí			2.5.4.3
1.6.6. Organization Identifier	No Aplica, No usado en ECI LETMI ECUADOR S.A.	No		Codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio	2.5.4.97
1.7. Subject Public Key Info		Sí			

1.7.1. AlgorithmIdentifier					
1.7.1.1. Algorithm	RSA encryption	Sí		1.2.840.113549.1.1.1	
1.7.1.2. Parameters	No aplicable	No			
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits	Sí			
2. Extensions					
2.1. Authority Key Identifier	Identificador de la clave del Issuer	No	No	(Marcado como NO Crítico según EN 319412-2) No es obligatorio siempre y cuando la clave pública de la AC se distribuye en forma de certificado “AUTOFIRMADO”	2.5.29.35
2.1.1. KeyIdentifier		No		Derivado de la clave pública	
2.2. Subject Key Identifier	Identificador de la clave del subject	Sí	No	(Marcado como NO Crítico según EN 319412-2)	2.5.29.14
2.2.1. KeyIdentifier		Sí		Derivado de la clave pública	
2.3. Key Usage		Sí	Sí		2.5.29.15
2.3.1. Digital Signature	Seleccionado “1”	Sí			
2.3.2. Content commitment	Seleccionado “1”	Sí			
2.3.3. Key Encipherment	No seleccionado. “0”				
2.3.4. Data Encipherment	No seleccionado. “0”				
2.3.5. Key Agreement	No seleccionado. “0”				
2.3.6. Key Certificate Signature	No seleccionado. “0”				
2.3.7. CRL Signature	No seleccionado. “0”				
2.3.8. Encipher Only	No seleccionado. “0”				
2.3.9. Decipher Only	No seleccionado. “0”				
2.4. Certificate Policies		Sí	No	(Marcado como NO Crítico según EN 319412-2)	2.5.29.32
2.4.1. Policy Information		Sí			
2.4.1.1. Policy Identifier	1.3.6.1.4.1.62566.2.6.1	Sí		Identificador de la política de la AC	
2.4.1.2. Policy Qualifiers		Sí			
2.4.1.1.1. CPS URI	https://letmi.app/documentos/Marco_regulatorio/DPC/Declaracion_de_Practicas_de_Certificacion_V1pdf	Sí		URL de la Política de Certificados de la Entidad Acreditada	1.3.6.1.5.5.7.2.1
2.4.1.1.2. User Notice/Explicit text	"CERTIFICADO DE VALIDACIÓN OCSP"	Sí		Texto indicativo	1.3.6.1.5.5.7.2.2
2.5. Subject Alternative Names		Sí	No	(Marcado como NO Crítico según EN 319412-2)	2.5.29.17
2.5.1. rfc822Name	Correo electrónico de la Entidad Acreditada "info@letmi.app"	Sí			
2.6. Extended Key Usage		Sí	No	(Marcado como NO Crítico según EN 319412-2)	2.5.29.37
2.6.1. ocspSigning	Presente (1.3.6.1.5.5.7.3.9)	Sí		Transport Layer Security (TLS) World Wide Web (WWW) client authentication CERTIFICADO DE VALIDACIÓN OCSP - ANEXO 8	
2.6.2. ocspNoCheck	Presente (1.3.6.1.5.5.7.48.1.5)	Sí		Para validar el certificado OCSP, para no entrar en loop (debe ser NULL)	
2.7. cRLDistributionPoint		Sí	No	Marcado como NO Crítico según EN 319412-2	2.5.29.31
2.7.1. distributionPoint	https://crl.letmi.app/LETMI_CA_SUB01.crl	Sí		URL de acceso al CRL http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC4516 [4] scheme	
2.7.2. distributionPoint	No aplicable	No		URL de acceso al CRL http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC4516 [4] scheme	
2.8. Authority Information Access		No	No	(Marcado como NO Crítico según EN 319412-2)	1.3.6.1.5.5.7.1.1
2.8.1. Access Description		No		No es obligatorio, en este caso al ser un certificado de OCSP no puede entrar en autovalidación	
2.8.1.1. Access Method	id-ad-calssuers	No			1.3.6.1.5.5.7.48.2
2.8.1.1.1. Access Location	No Aplica	No		URL acceso a certificado de la AC (http://) IETF RFC 7230-7235 [3] o	

				https (https:// IETF RFC 2818 [5]	
2.10. Basic Constraints		Sí	Sí		2.5.29.19
2.10.1. cA	FALSE	Sí			

1.2.3. Políticas asignadas a este documento.

Este documento en concreto da respuesta a las PC de los siguientes certificados :

- Letmi- Certificados de validación OCSP

1.3. Participantes PKI.

1.3.1. Autoridad de Certificación (CA).

Es aquella persona jurídica, acreditada conforme a la la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos "Ley N°67 del 2002" y el Decreto 3496 de 2002, facultada por el gobierno Ecuatoriano o ARCOTEL para prestar servicios de certificación digital de acuerdo a lo establecido en la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos "Ley N°67 del 2002", el Decreto 3496 de 2002 y los reglamentos que los modifiquen o complementen, es el origen de la jerarquía de certificación digital que le permite prestar los servicios relativos a las comunicaciones basadas en infraestructuras de clave pública.

1.3.2. Autoridad de Registro (RA).

Es el área de Letmi Ecuador S.A encargada de certificar la validez de la información suministrada por el solicitante de un servicio de certificación digital, mediante la verificación de la entidad del titular de la firma o responsable de los servicios de certificación digital, en la RA se decide sobre la emisión o activación del servicio de certificación digital. Para ello, tiene definidos los criterios y métodos de evaluación de solicitudes.

Bajo esta PC, la figura de RA hace parte de la propia ECI y podrá actuar como Subordinada de ECI Letmi Ecuador S.A.

Letmi Ecuador S.A en ninguna circunstancia delega las funciones de Autoridad de Registro (RA).

1.3.3. Titular de la firma y/o responsable.

Titular de la firma es la persona natural a la cual se emiten o activan los servicios de certificación digital y por tanto actúa como titular de la firma o responsable del mismo confiando en él, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en esta DPC.

La figura de titular de la firma será diferente dependiendo de los servicios prestados por la ECI Letmi Ecuador S.A conforme lo establecido en las Políticas de Certificado para certificados digitales.

1.3.4. Tercero de buena fe.

Responsable es la persona natural a la cual se activan los servicios de certificación digital de una persona jurídica y por tanto actúa como responsable de este confiando en él, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en esta DPC.

La figura de responsable será diferente dependiendo de los servicios prestados por la ECI Letmi Ecuador S.A conforme lo establecido en el Anexo 1 de esta DPC.

1.3.4.1. Precauciones que deben observar los terceros:

1. Verificar el alcance del certificado en la política de certificación asociada.
2. Consulte la normatividad asociada a los servicios de certificación digital
3. Verificar el estatus de acreditación de la ECI ante ARCOTEL.
4. Verificar que la firma digital se generó correctamente.
5. Verificar el origen del certificado (Cadena de certificación)
6. Verificar su conformidad con el contenido del certificado.
7. Verificar la integridad de un documento firmado digitalmente.

1.3.5. Solicitante.

Se entenderá por Solicitante, la persona natural o jurídica interesada en los servicios de certificación digital emitidos bajo esta PC. Puede coincidir con la figura del titular de la firma.

1.3.6. Entidad a la cual se encuentra vinculado el titular de la firma o responsable.

En su caso, la persona jurídica u organización a la que el titular de la firma o responsable se encuentra estrechamente relacionado mediante la vinculación acreditada en el servicio de certificación digital.

1.3.7. Otros participantes.

1.3.7.1. Comité de Gerencia.

El comité de Gerencia es un organismo interno de ECI Letmi Ecuador S.A, que está conformado de acuerdo con el reglamento del comité de gerencia quienes tienen la responsabilidad de la aprobación de la DPC como documento inicial, así como autorizar los cambios o modificaciones requeridas sobre la DPC aprobada y autorizar su publicación.

1.3.7.2. Proveedores de servicios.

Los proveedores de servicios son terceros que prestan infraestructura o servicios tecnológicos a ECI Letmi Ecuador S.A, cuando Letmi Ecuador S.A así lo requiere y garantiza la continuidad del servicio a los titular de la firma, entidades durante todo el tiempo en que se hayan contratado los servicios de certificación digital.

1.3.7.3. Entidades de Certificación de Información Reciprocas.

De acuerdo con lo previsto la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos "Ley N°67 del 2002" y el Decreto 3496 de 2002, los certificados electrónicos emitidos por entidades de certificación extranjeras, que cumplieren con los requisitos señalados en esta Ley y presenten un grado de fiabilidad equivalente, tendrán el mismo valor legal que los certificados acreditados, expedidos en el Ecuador. El Consejo Nacional de Telecomunicaciones dictará el reglamento correspondiente para la aplicación de este artículo.
Las firmas electrónicas creadas en el extranjero, para el reconocimiento de su validez en el Ecuador se someterán a lo previsto en esta Ley y su reglamento.

Actualmente ECI **Letmi Ecuador S.A** no cuenta con acuerdos vigentes de reciprocidad.

1.3.7.4. Peticiones, Quejas, Reclamos y Solicitudes.

Las peticiones, quejas, reclamos y solicitudes sobre los servicios prestados por ECI Letmi Ecuador S.A o entidades subcontratadas, explicaciones sobre esta Política de Certificación; son recibidas y atendidas directamente por Letmi Ecuador S.A como ECI y serán resueltas por las personas pertinentes e imparciales o por los comités que tengan la competencia técnica necesaria, para lo cual se disponen de los siguientes canales para la atención a titular de la firma, responsables y terceros.

Teléfono:	+59 (3) 02 2435200 (principal) +59 (3) 02 2921948 (alterno)
Correo electrónico:	pqrs@letmi.app
Dirección:	Calle Corea #126 Av Amazonas Edificio Belmonte Oficina 5 Piso 5
Página Web:	https://letmi.app/
Responsable:	Servicio al Cliente

Una vez presentado el caso, este es trasmitido con la información concerniente al proceso del Servicio al Cliente según procedimiento interno establecido para la investigación y gestión de estas. Del mismo modo, se determina qué área es responsable de tomar acciones correctivas o preventivas, caso en el cual se debe aplicar el procedimiento de acciones.

Generada la investigación se procede a evaluar la respuesta para posteriormente tomar la decisión que resuelve la PQRS y su comunicación final al titular de la firma, responsable o parte interesada.

1.4. Descripción de los Servicios de Validación

Los Servicios de Validación de Letmi Ecuador S.A permiten verificar la validez de los certificados electrónicos, y también cuenta con una aplicación que facilita la comprobación de la integridad y autenticidad de los certificados emitidos por Letmi Ecuador S.A

Letmi Ecuador S.A pone a disposición varios servicios de validación:

• **Servicio OCSP.**

Es una infraestructura distribuida de Respondedores OCSP que realizan consultas en tiempo real y de manera directa sobre los repositorios de la entidad emisora. Las respuestas OCSP están electrónicamente firmadas y cumplen con la norma IETF RFC 6960, X.509, Protocolo de Estado de Certificado en Línea de la Infraestructura Pública de Claves en Internet – OCSP.

Los campos opcionales según lo especificado en la RFC 6960:

Campo	Definición
CertID.hashAlgorithm	Identificador del algoritmo hash
CertID. issuerNameHash	Hash del DN del emisor (OCTET STRING)
CertID.serialNumber	Número de serie del certificado que se desea validar
CertID. issuerKeyHash	Hash de la clave pública del emisor (OCTET STRING)
nonce	Opcional
certReq	Todas las respuestas contienen la cadena de certificación de Letmi Ecuador S.A hasta la raíz. Su presencia y valor es ignorada.

1.5. Administración de Políticas.

La administración de las Políticas de Certificación (PC) estarán a cargo del proceso de Operaciones:

1.5.1. Persona de contacto:

Cargo del contacto:	Apoderado
Teléfonos de contacto:	+59 (3) 02 2435200 (principal) +59 (3) 02 2921948 (alterno)
Correo electrónico:	info@letmi.app

1.5.2. Procedimiento de aprobación de las Políticas

Las políticas deben ser aprobadas en todos los casos por el Comité de Gerencia.

1.5.3. Responsabilidades de publicación

Una vez realizado y aprobados los cambios de las políticas, es responsabilidad del Coordinador de Operaciones y/o el Proceso del Sistema Integrado de Gestión solicitar al proceso encargado la actualización en los portales WEB de las políticas en su última versión.

1.6. Definiciones y Siglas

1.6.1. Definiciones

Los siguientes términos son de uso común y requerido para el entendimiento de la presente Política.

Autoridad de Certificación (CA): En inglés "Certification Authority" (CA): Autoridad de Certificación, entidad raíz y entidad prestadora de servicios de certificación de infraestructura de llave pública.

Autoridad de Registro (RA): En inglés "Registration Authority" (RA): Es la entidad encargada de certificar la validez de la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro.

Autoridad de Sellado de Tiempo (TSA): Sigla en inglés de "Time Stamping Authority": Entidad de certificación prestadora de servicios de sellado de tiempo.

Archivo confiable de datos: Es el servicio que Letmi Ecuador S.A ofrece a sus clientes por medio de una plataforma tecnológica. En esencia, consiste en un espacio de almacenamiento seguro y encriptado al cual se accede con credenciales o con un certificado digital. La documentación que se almacene en esta plataforma tendrá valor probatorio siempre y cuando este firmada digitalmente.

Certificado digital: Un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

Clave Personal de Acceso (PIN): Sigla en inglés de "Personal Identification Number": Secuencia de caracteres que permiten el acceso al certificado digital.

Compromiso de la llave privada: entiéndase por compromiso el robo, pérdida, destrucción divulgación de la llave privada que pueda poner en riesgo el empleo y uso del certificado por parte terceros no autorizados o el sistema de certificación.

Correo electrónico certificado: Servicio que permite asegurar el envío, recepción y comprobación de comunicaciones electrónicas, asegurándose en todo momento las características de fidelidad, autoría, trazabilidad y no repudio de la misma.

Declaración de Prácticas de Certificación (DPC): En inglés "Certification Practice Statement" (CPS): manifestación de la entidad de certificación sobre las políticas y procedimientos que aplica para la prestación de sus servicios.

Dispositivo Seguro de Creación de Firma DSCF: Instrumento que sirve para aplicar los datos de creación de firma.

Entidad de Certificación de Información (ECI): Es aquella persona jurídica, acreditada conforme a la ley 67 de 2002 y el Decreto 3496 de 2002, facultadas por el gobierno Ecuatoriano (Agencia de Regulación y Control de las Telecomunicaciones) para emitir certificados en relación con las firmas digitales de los clientes que las adquieran, ofrecer o facilitar los servicios de registro y sellado de tiempo de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

Entidad de Certificación Abierta: Es una Entidad Certificación que ofrece servicios propios de las entidades de certificación, tales que:

1. Su uso no se limita al intercambio de mensajes entre la entidad y el titular de la firma, o
2. Recibe remuneración por éstos.

Entidad de certificación cerrada: Entidad que ofrece servicios propios de las entidades de certificación solo para el intercambio de mensajes entre la entidad y el titular de la firma, sin exigir remuneración por ello.

Infraestructura de Llave Pública (PKI): Sigla en inglés de "Public Key Infrastructure": una PKI es una combinación de hardware y software, políticas y procedimientos de seguridad que permite, a los usuarios de una red pública básicamente insegura como el Internet, el intercambio de mensajes de datos de una manera segura utilizando un par de llaves criptográficas (una privada y una pública) que se obtienen y son compartidas a través de una autoridad de confianza.

Iniciador: Persona que, actuando por su cuenta, o en cuyo nombre se haya actuado, envíe o genere un mensaje de datos.

Jerarquía de confianza: Conjunto de autoridades de certificación que mantienen relaciones de confianza por las cuales una ECI de nivel superior garantiza la confiabilidad de una o varias de nivel inferior.

Lista de Certificados Revocados (CRL): Sigla en inglés de "Certificate Revocation List": Lista donde figuran exclusivamente los certificados revocados no vencidos.

Llave Pública y Llave Privada: La criptografía asimétrica en la que se basa la PKI. Emplea un par de llaves en la que se cifra con una y solo se puede descifrar con la otra y viceversa. A una de esas llaves se la denomina pública y se incluye en el certificado digital, mientras que a la otra se denomina privada y es conocida únicamente por el titular de la firma o responsable del certificado.

Llave privada (Clave privada): Valor o valores numéricos que, utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos.

Llave pública (Clave pública): Valor o valores numéricos que son utilizados para verificar que una firma digital fue generada con la clave privada de quien actúa como iniciador.

Módulo Criptográfico Hardware de Seguridad: Sigla en inglés de "Hardware Security Module", módulo hardware utilizado para realizar funciones criptográficas y almacenar llaves en modo seguro.

Política de Certificación (PC): Es un conjunto de reglas que definen las características de los distintos tipos de certificados y su uso.

Prestador de Servicios de Certificación (PSC): En inglés "Certification Service Provider" (CSP): persona natural o jurídica que expide certificados digitales y presta otros servicios en relación con las firmas digitales.

Protocolo de Estado de los Certificados En-línea: En inglés "Online Certificate Status Protocol" (OCSP): Protocolo que permite verificar en línea el estado de un certificado digital

Repositorio: Sistema de información utilizado para almacenar y recuperar certificados y otra información relacionada con los mismos.

Revocación: Proceso por el cual un certificado digital se deshabilita y pierde validez.

Sellado de Tiempo: Según el Art 23 del Decreto 3496 de 2002, se define como: El sellado de tiempo únicamente establecerá para los fines legales pertinentes, la hora y fecha exacta en que el mensaje de datos fue recibido por la entidad certificadora o el tercero registrado por el CONATEL; y la fecha y hora exacta en dicho mensaje de datos fue entregado al destinatario.

Solicitante: Toda persona natural o jurídica que solicita la expedición o renovación de un Certificado digital.

Titular de la firma y/o responsable: Persona natural o jurídica a la cual se emiten o activan los servicios de certificación digital y por tanto actúa como titular de la firma o responsable del mismo

Tercero de buena fe: Persona o entidad diferente del titular de la firma y/o responsable que decide aceptar y confiar en un certificado digital emitido por ECI Letmi Ecuador S.A.

TSA Letmi Ecuador S.A: Corresponde al término utilizado por ECI Letmi Ecuador S.A, en la prestación de su servicio de sellado de tiempo, como Autoridad de sellado de tiempo.

1.6.2. Siglas

CA: Certification Authority

CPS: Certification Practice Statement

CRL: Certificate Revocation List

CSP: Certification Service Provider

DNS: Domain Name System

DSCF: Dispositivo Seguro de Creación de Firma

FIPS: Federal Information Processing Standard

HTTP: El protocolo de transferencia de hipertexto (HTTP, HyperText Transfer Protocol) es el protocolo usado en cada transacción de la Web (WWW). HTTP define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor.

HTTPS: Hypertext Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), más conocido por su acrónimo HTTPS, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.

IEC: International Electrotechnical Commission

IETF: Internet Engineering Task Force (Organismo de estandarización de Internet)

IP: Internet Protocol

ISO: International Organization for Standardization

OCSP: Online Certificate Status Protocol.

OID: Object identifier (Identificador de objeto único)

PIN: Personal Identification Number

PUK: Personal Unlocking Key

PKCS: Public Key Cryptography Standards. Estándares de PKI desarrollados por RSA Laboratories y aceptados internacionalmente.

PKI: Public Key Infrastructure (Infraestructura de Llave Pública)

PKIX: Public Key Infrastructure (X.509)

RA: Registration Authority

RFC: Request For Comments (Estándar emitido por la IETF)

URL: Uniform Resource Locator

1.7. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO.

1.7.1. Repositorios de la PKI.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

1.7.2. Publicación de la información de certificación.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

1.7.3. Plazo o frecuencia de la publicación.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

1.7.4. Controles de acceso a los repositorios.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

1.8. PROCEDIMIENTO DE VALIDACIÓN

El proceso de validación de un certificado electrónico que ha sido emitido por Letmi Ecuador S.A, es necesario seguir los procedimientos establecidos en el estándar RFC 5280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.. Al adherirse a este estándar, se podrá llevar a cabo la validación técnica de cualquier certificado electrónico. Para ello, se requiere:

- Contar con el certificado raíz de la autoridad certificadora emisora, disponible en el sitio web de Letmi Ecuador S.A: https://letmi.app/
- Tener a disposición una copia del certificado electrónico a validar, junto con su número de serie o el nombre del suscriptor.

La ECI-Letmi Ecuador S.A cuenta con un sistema de gestión de seguridad para proteger la información que se recopila con el fin de expedir los certificados el cual está establecido en la DPC en “Controles de seguridad informática”.

1.8.1. Servicios de Validación

- **Consulta OCSP**
  Las respuestas relativas a la validación de un certificado están firmadas por Letmi Ecuador S.A, lo que garantiza la obtención de una prueba electrónica de la respuesta generada, de acuerdo con la norma RFC 6960, Protocolo de Estado de Certificado en Línea – OCSP.

1.8.2. Usos permitidos

Los servicios de validación de Letmi Ecuador S.A. están destinados exclusivamente a satisfacer las necesidades de validación en calidad de suscriptor o de terceros que confían.

1.8.3. Usos prohibidos

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

1.9. PERFILES DE CERTIFICADO PERFILES DE CERTIFICADO OCSP.

1.9.1. Perfil OCSP.

De acuerdo con el numeral 1.2.2 OID de las políticas de este documento.

1.10.1. Obligaciones de la ECI Letmi Ecuador S.A

ECI Letmi Ecuador S.A como entidad de prestación de servicios de certificación está obligada según normativa vigente, en lo dispuesto en las Políticas de Certificado y en la DPC a:

1. Respetar lo dispuesto en la normatividad vigente, la DPC y en las Políticas de Certificado.
2. Publicar la DPC y cada una de las Políticas de Certificado en la página Web de Letmi Ecuador S.A.
3. Mantener la DPC y Políticas de Certificado con su última versión publicadas en la página Web de Letmi Ecuador S.A.
4. Proteger y custodiar de manera segura y responsable su llave privada.
5. Emitir certificados conforme a las Políticas de Certificado y a los estándares definidos en la DPC.
6. Generar certificados consistentes con la información suministrada por el solicitante o titular de la firma.
7. Conservar la información sobre los certificados digitales emitidos de conformidad con la normatividad vigente.
8. Emitir certificados cuyo contenido mínimo este de conformidad con la normativa vigente para los diferentes tipos de certificados.
9. Publicar el estado de los certificados digitales emitidos en un repositorio de acceso libre.
10. No mantener copia de la llave privada del solicitante o titular de la firma.
11. Actualizar y publicar la lista de certificados digitales cancelados CRL con los últimos certificados cancelados.
12. Notificar al Solicitante, titular de la firma o Entidad la cancelación del certificado digital dentro de las 24 horas siguientes a la cancelación del certificado digital.

13. Informar a los titular de la firma la proximidad del vencimiento de su certificado digital.
14. Disponer de personal calificado, con el conocimiento y experiencia necesaria para la prestación del servicio de certificación ofrecido por la ECI Letmi Ecuador S.A.
15. Proporcionar al solicitante en la página web de la ECI Letmi Ecuador S.A la siguiente información de manera gratuita y acceso libre:
    - Las Políticas y Declaración de Prácticas de certificación y todas sus actualizaciones.
    - Obligaciones del titular de la firma y la forma en que han de custodiarse los datos
    - Procedimiento para solicitar la emisión de certificado.
    - Mecanismos para garantizar la fiabilidad de la firma electrónica a lo largo del tiempo.
    - Las condiciones y límites del uso del certificado
16. Comprobar por sí o por medio de una persona diferente que actúe en nombre y por cuenta suya, la identidad y cualesquiera otras circunstancias de los solicitantes o de datos de los certificados, que sean relevantes para los fines propios del procedimiento de verificación previo a su expedición.
17. Informar al ARCOTEL, de manera inmediata, la ocurrencia de cualquier evento que comprometa o pueda comprometer la prestación del servicio.
18. Informar oportunamente la modificación o actualización de servicios incluidos en el alcance de su acreditación, en los términos que establezcan los procedimientos, reglas y requisitos del servicio de acreditación del ARCOTEL.
19. Actualizar la información de contacto cada vez que haya cambio o modificación en los datos suministrados.
20. Capacitar y advertir a sus usuarios sobre las medidas de seguridad que deben observar y sobre la logística que se requiere para la utilización de los mecanismos de la prestación del servicio.
21. Garantizar la protección, integridad, confidencialidad y seguridad de la información suministrada por el titular de la firma conservando la documentación que respalda los certificados emitidos.
22. Garantizar las condiciones de integridad, disponibilidad, confidencialidad y seguridad, de acuerdo con los estándares técnicos nacionales e internacionales vigentes y con los criterios específicos de acreditación que para el efecto establezca el ARCOTEL.
23. Disponer en la página web de la ECI Letmi Ecuador S.A los servicios que se encuentran acreditados.

1.10.2. Obligaciones de la RA

La RA de la ECI Letmi Ecuador S.A está facultada para realizar la labor de identificación y registro, por lo tanto, está obligada en los términos definidos en la Declaración de Prácticas de Certificación a:

1. Conocer y dar cumplimiento a lo dispuesto en la DPC y en la Política de Certificado correspondiente a cada tipo de certificado.
2. Custodiar y proteger su llave privada.
3. Revisar y/o comprobar los registros de validación inicial de la identidad de los Solicitantes, Responsables o titular de la firma de certificados digitales.
4. Verificar la exactitud y autenticidad de la información suministrada por el Solicitante mediante los protocolos descritos en la DPC
5. Archivar y custodiar la información y/o documentación suministrada por el solicitante o titular de la firma para la emisión del certificado digital, durante el tiempo establecido por la legislación vigente.
6. Respetar lo dispuesto en los contratos firmados entre ECI Letmi Ecuador S.A y el titular de la firma.
7. Identificar e informar a la ECI Letmi Ecuador S.A las causas de cancelación suministradas por los solicitantes sobre los certificados digitales vigentes.

1.10.3. Obligaciones (Deberes y Derechos) del titular de la firma y/o Responsable

El titular de la firma y/o Responsable de un certificado digital está obligado a cumplir con lo dispuesto por la normativa vigente y lo dispuesto en la DPC como es:

1. Usar su certificado digital según los términos de la DPC.
2. Verificar dentro del día siguiente hábil que la información del certificado digital es correcta. En caso de encontrar inconsistencias, notificar a la ECI.
3. Abstenerse de: prestar, ceder, escribir, publicar la contraseña de uso su certificado digital y tomar todas las medidas necesarias, razonables y oportunas para evitar que éste sea utilizado por terceras personas.
4. No transferir, compartir ni prestar el dispositivo criptográfico a terceras personas.
5. Suministrar toda la información requerida en el Formulario de la Solicitud para facilitar su oportuna y plena identificación.
6. Solicitar la cancelación del Certificado Digital ante el cambio de nombre y/o apellidos.
7. Solicitar la cancelación del Certificado Digital cuando el titular de la firma haya variado su nacionalidad.
8. Cumplir con lo aceptado y firmado en el documento términos y condiciones o responsable de certificados digitales.
9. Proporcionar con exactitud y veracidad la información requerida.
10. Informar durante la vigencia del certificado digital cualquier cambio en los datos suministrados inicialmente para la emisión del certificado.
11. Custodiar y proteger de manera responsable su llave privada.
12. Dar uso al certificado de conformidad con lo establecido en esta PC para cada uno de los tipos de certificado.
13. Solicitar como titular de la firma o responsable de manera inmediata la cancelación de su certificado digital cuando tenga conocimiento que existe una causal definida en numeral *Circunstancias para la cancelación de un certificado* de la DPC.
14. No hacer uso de la llave privada ni del certificado digital una vez cumplida su vigencia o se encuentre cancelado.
15. Informar a los terceros de confianza de la necesidad de comprobar la validez de los certificados digitales sobre los que esté haciendo uso en un momento dado.
16. Informar al tercero de buena fe para verificar el estado de un certificado dispone de la lista de certificados revocados CRL, publicada de manera de periódica por ECI Letmi Ecuador S.A.
17. No utilizar su certificación digital de manera que contravenga la ley u ocasione mala reputación para la ECI.
18. No realizar ninguna declaración relacionada con su certificación digital en la ECI Letmi Ecuador S.A pueda considerar engañosa o no autorizada, conforme a lo dispuesto por la DPC y PC.
19. Una vez caducado el servicio de certificación digital el titular de la firma debe inmediatamente dejar de utilizarla en todo el material publicitario que contenga alguna referencia al servicio.
20. El titular de la firma al hacer referencia al servicio de certificación digital prestado por ECI Letmi Ecuador S.A en medios de comunicación, tales como documentos, folletos o publicidad, debe informar que cumple con los requisitos especificados en las PC de la DPC, indicando la versión.
21. El titular de la firma podrá utilizar las marcas de conformidad y la información relacionada con el servicio de certificación digital prestado por ECI Letmi Ecuador S.A en medios de comunicación, tales como documentos, folletos o publicidad, desde que cumpla lo requerido en el literal anterior.

Por otro lado, tiene los siguientes derechos:

1. Recibir el certificado digital en los tiempos establecidos en la DPC.
2. El titular de la firma podrá utilizar las marcas de conformidad y la información relacionada con el servicio de certificación digital prestado por ECI Letmi Ecuador S.A en medios de comunicación, tales como documentos, folletos o publicidad, desde que cumpla lo requerido en el literal anterior.
3. Solicitar información referente a las solicitudes en proceso.
4. Solicitar cancelación del certificado digital aportando la documentación necesaria.
5. Recibir el certificado digital de acuerdo con el alcance otorgado por ARCOTEL a Letmi Ecuador S.A.

1.10.4. Obligaciones de los Terceros de buena fe

Los Terceros de buena fe en su calidad de parte que confía en los certificados digitales emitidos por ECI Letmi Ecuador S.A está en la obligación de:

1. Conocer lo dispuesto sobre Certificación Digital en la Normatividad vigente.
2. Conocer lo dispuesto en la DPC y PC.
3. Verificar el estado de los certificados antes de realizar operaciones con certificados digitales.
4. Verificar la Lista de certificados Revocados CRL antes de realizar operaciones con certificados digitales.
5. Conocer y aceptar las condiciones sobre garantías, usos y responsabilidades al realizar operaciones con certificados digitales.

1.10.5. Obligaciones de la Entidad (Cliente)

La entidad cliente es la encargada de solicitar los servicios para sus funcionarios y los titular de la firma son las personas que hacen uso del servicio.

Conforme lo establecido en las Políticas de Certificado, en el caso de los certificados donde se acredite la vinculación del titular de la firma o Responsable con la misma, será obligación de la Entidad:

1. Solicitar a la RA Letmi Ecuador S.A la suspensión/cancelación del certificado cuando cese o se modifique dicha vinculación.
2. Todas aquellas obligaciones vinculadas al responsable del servicio de certificación digital.
3. La entidad al hacer referencia al servicio de certificación digital prestado por ECI Letmi Ecuador S.A en medios de comunicación, tales como documentos, folletos o publicidad, debe informar que cumple con los requisitos especificados en las PC de la DPC.
4. La entidad podrá utilizar las marcas de conformidad y la información relacionada con el servicio de certificación digital prestado por ECI Letmi Ecuador S.A en medios de comunicación, tales como documentos, folletos o publicidad, desde que cumpla lo requerido en el literal anterior.

1.10.6. Obligaciones de otros participantes de la ECI

El Comité de Gerencia y el proceso Sistema Integrado de Gestión como organismos internos de ECI Letmi Ecuador S.A está en la obligación de:

1. Revisar la consistencia de la DPC con la normatividad vigente.
2. Aprobar y decidir sobre los cambios a realizar sobre los servicios de certificación digital, por decisiones de tipo normativo o por solicitudes de titular de la firma o responsables.
3. Aprobar la notificación de cualquier cambio a los titular de la firma y/o responsables analizando su impacto legal, técnico o comercial.
4. Revisar y tomar acciones sobre cualquier comentario realizado por titular de la firma y/o responsables cuando un cambio en el servicio de certificación digital se realice.
5. Autorizar los cambios o modificaciones requeridas sobre la DPC.
6. Autorizar la publicación de la DPC en la página Web de la ECI Letmi Ecuador S.A.
7. Aprobar los cambios o modificaciones a las Políticas de Seguridad de la ECI Letmi Ecuador S.A.
8. Asegurar la integridad y disponibilidad de la información publicada en la página Web de la ECI Letmi Ecuador S.A
9. Asegurar la existencia de controles sobre la infraestructura tecnológica de la ECI Letmi Ecuador S.A.
10. Solicitar la cancelación de un certificado si tuviera el conocimiento o sospecha del compromiso de la llave privada del titular de la firma, entidad o cualquier otro hecho que tienda al uso indebido de llave privada del titular de la firma, entidad o de la propia ECI.
11. Conocer y tomar acciones pertinentes cuando se presenten incidentes de seguridad.
12. Realizar con una frecuencia máxima anual, una revisión de la DPC para verificar que las longitudes de las llaves y periodos de los certificados que se estén empleando son adecuados.
13. Revisar, aprobar y autorizar cambios sobre los servicios de certificación digital acreditados por el organismo competente.
14. Revisar, aprobar y autorizar la propiedad y el uso de símbolos, certificados y cualquier otro mecanismo que requiera ECI Letmi Ecuador S.A para indicar que el servicio de certificación digital está acreditado.
15. Velar que las condiciones de acreditación otorgado por el organismo competente se mantengan.
16. Velar por el uso adecuado en documentos o en cualquier otra publicidad que los símbolos, los certificados, y cualquier otro mecanismo que indique que ECI **Letmi Ecuador S.A** cuenta con un servicio de certificación acreditado y cumple con lo dispuesto en la la RESOLUCIÓN ARCOTEL-2024-0176 del 16 de agosto de 2024.
17. Velar por mantener informados a sus proveedores críticos y ECI recíproca en caso de existir, de la obligación de cumplimiento de los requisitos de la la RESOLUCIÓN ARCOTEL-2024-0176 del 16 de agosto de 2024, en los numerales que correspondan.
18. El proceso del Sistema Integrado de Gestión ejecutará planes de acción preventivos y correctivos para responder ante cualquier riesgo que comprometa la imparcialidad y no discriminación de la ECI, ya sea que se derive de las acciones de cualquier persona, organismo, organización, actividades, sus relaciones o las relaciones de su personal o de sí misma. Para lo cual utiliza la norma ISO 31000 para la identificación de riesgos que comprometa la imparcialidad de la ECI.
19. Velar que todo el personal y los comités de la ECI (sean internos o externos), que puedan tener influencia en las actividades de certificación actúen con imparcialidad y no discriminación, especialmente aquellas que surjan por presiones comerciales, financieras u otras comprometan su imparcialidad.
20. Documentar y demostrar el compromiso de imparcialidad y no discriminación.
21. Velar que el personal administrativo, de gestión, técnico de la PKI, de la ECI asociado a las actividades de consultoría, mantenga completa independencia y autonomía respecto al personal del proceso de revisión y toma de decisión sobre la certificación de la misma ECI.
22. Velar por mantener informados a sus proveedores críticos como la ECI reciproca y datacenter que cumplen con los requisitos de acreditación para ECI como soporte para su contratación y del cumplimiento de los requisitos solicitados tanto administrativos como técnicos.

1.10.7. Enmiendas.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

1.10.8. Procedimientos de Resolución de Disputas.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

1.10.9. Ley Aplicable.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

2. PERFIL DE LOS CERTIFICADOS

Consultar el Anexo 1 de la DPC Matriz Perfil Técnico de los Certificados

OID (Object Identifier)	1.3.6.1.4.1.62566.2.6.1
Ubicación de la PC	https://letmi.app/documentos/Marco_regulatorio/politicas/Politicas_de_Certificados_de_validación_OCSP_V1.pdf

Firma Apoderado

Letmi Ecuador S.A