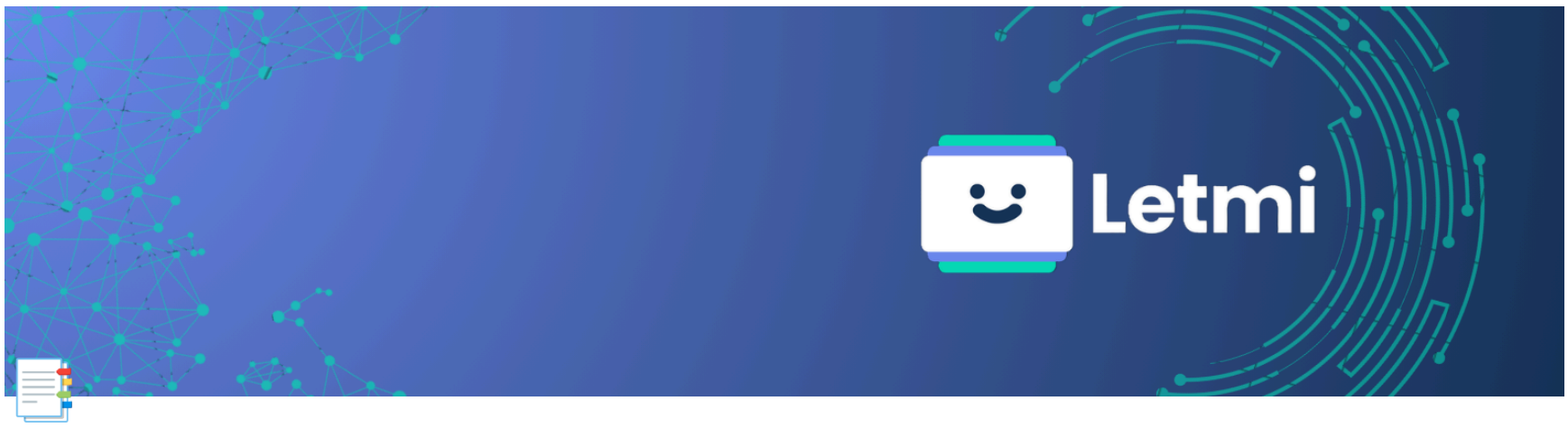


Declaración de Prácticas de Certificación V.5

La consulta a los repositorios disponibles en la página Web de **Letmi Ecuador S.A** antes mencionados, es de libre acceso al público en general. La integridad y disponibilidad de la información publicada es responsabilidad de ECI **Letmi Ecuador S.A** , que cuenta con los recursos y procedimientos necesarios para restringir el acceso a los repositorios con otros fines diferentes a la consulta.

Código	Nombre	Versión	Clasificación de la información
POP-DT-60	Declaración de Practicas de Certificación	5	Pública

Título del Documento	**Declaración de Prácticas de Certificación**
Versión	5
Grupo de Trabajo	Comité de Gerencia
Estado del documento	Final
Fecha de emisión	27/01/2025
Fecha de inicio de vigencia	21/04/2026
OID (Object Identifier) - IANA	1.3.6.1.4.1.62566.1.1.5
Ubicación de la DPC	https://letmi.app/documentos/Marco_regulatorio/DPC/Declaracion_de_Practicas_de_Certificacion_V5.pdf
Elaboró	Coordinador de Operaciones
Revisó	Sistema Integrado de Gestión
Aprobó	Apoderado

Control de Cambios

Versión	Fecha	Cambio/Modificación
1	27/01/2025	Documento inicial
2	03/09/2025	Se ajusta número de contacto de la ECI
3	16/02/2026	Se ajustan los siguientes numerales: • 1.3.1 Autoridad de Certificación (AC): Cambio del datacenter y datos de ubicación del mismo. • 7.1 Perfil del Certificado: En la tabla “Datos capturados en la solicitud” se adicionan las columnas para los tipos de certificado Sello Electrónico -SE (En Archivo), Persona Natural - PN (En Archivo) y Representante Legal - RL (En Archivo). • Políticas de certificación: Ajuste en el nombre de las políticas de acuerdo a la adición de nuevo formato en archivo. • Se agregan campos de firma de elaboró, revisó y aprobó al final del documento.
4	27/03/2026	Se ajustan los siguientes numerales: • 1. 2 Nombre e identificación del documento: Se incluyeron ajustes tales como el nombre exacto de la DPC, el OID único asignado, el número de versión, el historial de cambios, la fecha de aprobación interna, la fecha de publicación en el repositorio, el estado del documento (vigente) y la URL actualizada para el acceso público a la versión vigente del documento. •2.4 Control de Acceso: Se incorpora una descripción detallada de los controles implementados por la entidad. En este sentido, se incluyeron de manera explícita los mecanismos de control de acceso. Asimismo, se integraron los mecanismos orientados a garantizar la integridad de la información, junto con la definición de compromisos formales relacionados con la revisión periódica y auditoría de dichos controles, con el fin de asegurar su adecuada implementación y efectividad. • 3. Identificación y Autenticación: Se amplia la descripción detallada de los procesos aplicables según el tipo de certificado emitido. Asimismo, se incluyeron los mecanismos de identificación y autenticación correspondientes, junto con la especificación del mecanismo criptográfico utilizado en cada caso. • 4.5 Uso de pares de claves y certificados: Se incluyeron los tamaños de clave utilizados, así como los algoritmos hash aplicables. Adicionalmente, se definieron las condiciones relacionadas con la generación y almacenamiento de la clave privada, estableciendo el uso de dispositivos seguros, como módulos de seguridad hardware (HSM). • 8.2 Identidad y cualificaciones del evaluador: Se actualizó el numeral incorporando la especificación de

		que la entidad evaluadora o de inspección debe contar con la debida acreditación otorgada por el organismo nacional de acreditación competente, así como su reconocimiento por parte de la autoridad de control correspondiente. • 8.6 Comunicación de resultados: Se ajusta el numeral incorporando de manera expresa el plazo de quince (15) días hábiles para el envío correspondiente, contado a partir de la finalización del proceso, en cumplimiento de la normativa técnica vigente de ARCOTEL.. • 9.1 Tarifas: Se incorpora un detalle completo, desglosado y de acceso público de los costos asociados a los servicios ofertados, incluyendo la emisión, renovación, revocación, consulta y demás servicios relacionados incluyendo la estructura de precios correspondiente y las condiciones de pago aplicables. • 9.4 Privacidad de la Información personal: Se actualizó la sección 9.4 incorporando de manera expresa los derechos del titular de los datos personales, incluyendo acceso, rectificación y supresión, conforme a la terminología establecida en la normativa aplicable la Ley Orgánica de Protección de Datos Personales (LOPDP). Asimismo, se incluyeron los plazos de retención de la información personal una vez expirado el certificado. • 9.8 Limitaciones de Responsabilidad: Se adicionan las condiciones correspondientes a la garantía contratada por Letmi Ecuador S.A detallando adicionalmente el monto por el cual se contrató la misma y las condiciones de reclamación.
5	21/04/2026	• Se modifica diseño del documento. • Se amplía el servicio de certificación mediante la incorporación, en el presente documento, de los certificados para miembros de empresa o empleados en relación de dependencia, tanto en formato archivo como en dispositivo seguro de creación de firma (DSCF). • Subsanación de las observaciones emitidas por ARCOTEL ,mediante el Oficio Nro. ARCOTEL-CTDS-2026-0453-OF.

Tabla de Contenido

1. INTRODUCCIÓN.
  1.1 Descripción General
  1.2 Nombre e identificación del documento.
  1.3 Participantes PKI.
    1.3.1 Autoridad de Certificación (AC).
    1.3.2 Autoridad de Registro (AR).
    1.3.3 Suscriptor
    1.3.4 Partes de confianza.
    1.3.5 Otros participantes.
  1.4 Uso del certificado.
    1.4.1 Uso permitido de los certificados
      1.4.1.1 Uso permitido **del certificado de Persona Natural en DSCF y en archivo**
      1.4.1.2 Uso permitido **del certificado de Sello electrónico en DSCF y en archivo**
      1.4.1.3 Uso permitido **del certificado de Representante legal en DSCF y en archivo**
      1.4.1.4 Uso permitido del certificado de Miembro empresa o en relación de dependencia en DSCF y en archivo
    1.4.2 Uso prohibido de los certificados
      1.4.2.1 Uso prohibido del certificado de Persona Natural en DSCF y en archivo
      1.4.2.2 Uso prohibido del certificado de Sello Electrónico en DSCF y en archivo
      1.4.2.3 Uso prohibido del certificado de Representante Legal en DSCF y en archivo
      1.4.2.4 Uso prohibido del certificado de Miembro empresa o en relación de dependencia en DSCF y en archivo
  1.5 Administración de políticas.
    1.5.1 Organización que administra el documento.
    1.5.2 Contacto (Responsable de la ECI):
    1.5.3 Persona que determina la idoneidad de la DPC para la póliza.
    1.5.4 Procedimientos de aprobación de la DPC.
  1.6 Definiciones y acrónimos.
    Definiciones.
    Acrónimos.
    Estándares y Organismos de estandarización.
2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO.
  2.1 Repositorios.
  2.2 Publicación de información sobre certificación.
  2.3 Plazo o frecuencia de la publicación.
  2.4 Controles de acceso a los repositorios.
3. IDENTIFICACIÓN Y AUTENTICACIÓN.
  3.1 Nombres.
    3.1.1 Tipos de nombres.
    Certificados Raíz de la ECI Letmi Ecuador S.A.
    Certificados de las Subordinadas ECI Letmi Ecuador S.A.
    3.1.2 Necesidad de que los nombres tengan sentido.
    3.1.3 Anonimato o seudonimato de los titulares de la firma.
    3.1.4 Reglas de interpretación de las distintas formas del nombre.
    3.1.5 Unicidad de los Nombres.
    3.1.6 Reconocimiento, autenticación y rol de las marcas registradas.
  3.2 Validación inicial de identidad.
    3.2.1 Método para demostrar la posesión de la clave privada.
    3.2.2 Autenticación de la identidad de la organización.
    3.2.3 Autenticación de la identidad individual.
    3.2.4 Información de suscriptor no verificada.
    3.2.5 Validación de la autoridad.
    3.2.6 Criterios de interoperabilidad.
  3.3 Identificación y Autenticación para renovación de llaves.
    3.3.1 Identificación y autenticación para la renovación de claves rutinarias.
    3.3.2 Identificación y autenticación para la rutina de re-uso llaves tras la revocación.
  3.4 Identificación y autenticación para la solicitud de revocación.

4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DEL CERTIFICADO.
4.1 Solicitud de certificado.
4.1.1 Quién puede presentar una solicitud de certificado.
4.1.2 Proceso de inscripción y responsabilidades.
4.2 Procesamiento de solicitudes de certificado.
4.2.1 **Realizar funciones de identificación y autenticación.**
4.2.2 Aprobación o rechazo de solicitudes de certificado
4.2.3 Tiempo para procesar las solicitudes de certificado
4.3 Emisión del Certificado.
4.3.1 Acciones de la AC durante la emisión de certificados.
4.3.2 Notificación al suscriptor por parte de la AC de la emisión del certificado
4.4 Aceptación del Certificado.
4.4.1 **Conducta que constituye la aceptación del certificado.**
4.4.2 Publicación del certificado por la AC.
4.4.3 Notificación de la emisión de certificados por parte de la AC a otras entidades.
4.5 Uso de pares de claves y certificados.
4.5.1 Uso de la clave privada y el certificado del suscriptor.
4.5.2 Uso de certificados y claves públicas del tercero que confía.
4.6 Renovación del certificado
4.6.1 Circunstancias para la renovación de certificado.
4.6.2 Quién puede solicitar una renovación sin cambio de llaves.
4.6.3 Trámites para la solicitud de renovación de certificados.
4.6.4 Notificación al suscriptor o responsable de la emisión de un nuevo certificado sin cambio de llaves.
4.6.5 Forma en la que se acepta la renovación de un certificado.
4.6.6 Publicación del certificado renovado por la ECI.
4.6.7 Notificación de la emisión de un certificado renovado por la ECI a otras entidades.
4.7 Re-uso de clave del certificado
4.7.1 Circunstancia para el re-uso de claves del certificado.
4.7.2 Quién puede solicitar la certificación de una nueva clave pública.
4.7.3 Procesamiento de las solicitudes de re-uso de clave de certificados.
4.7.4 Notificación al suscriptor de la emisión de un nuevo certificado.
4.7.5 Conducta que constituye la aceptación de un certificado con re-uso de clave.
4.7.6 Publicación del certificado con re-uso de clave por parte de la AC
4.7.7 Notificación de la emisión de certificados por parte de la AC a otras entidades
4.8 Modificación del Certificado.
4.8.1 Circunstancias para la modificación del certificado.
4.8.2 Quién puede solicitar la modificación del certificado.
4.8.3 Tramitación de solicitudes de modificación de certificados.
4.8.4 Notificación al suscriptor de la emisión de un nuevo certificado
4.8.5 Conducta que constituye la aceptación de un certificado modificado.
4.8.6 Publicación del certificado modificado por la AC.
4.8.7 Notificación de la emisión de certificados por parte de la AC a otras entidades.
4.9 Revocación y suspensión del certificado.
4.9.1 Circunstancias para revocación.
4.9.2 Quién puede solicitar la revocación de un certificado.
4.9.3 Procedimiento para solicitud de revocación de un certificado.
4.9.4 Periodo de gracia para solicitar revocación de un certificado.
4.9.5 Tiempo dentro del cual la AC debe procesar la solicitud de revocación.
4.9.6 Requisito de comprobación de revocación para las partes confiantes.
4.9.7 Frecuencia de emisión de las CRLs.
4.9.8 Latencia máxima de las CRLs.
4.9.9 Disponibilidad de verificación en línea de revocación/estado.
4.9.10 Requisitos de comprobación de revocación en línea.
4.9.11 Otras formas de anuncios de revocación disponibles.
4.9.12 Requisitos especiales en materia de compromiso de claves.
4.9.13 Circunstancias para la suspensión
4.9.14 Quién puede solicitar la suspensión
4.9.15 Procedimiento de solicitud de suspensión
4.9.16 Límites del periodo de suspensión
4.10 Servicios de Estado de los Certificados.
4.10.1 Características operativas
4.10.2 Disponibilidad servicio
4.10.3 Características opcionales.
4.11 Fin de la Suscripción.
4.12 Custodia y Recuperación de claves
4.12.1 Política y prácticas en materia de custodia y recuperación de llaves.
4.12.2 Política y prácticas de encapsulación y recuperación de claves de sesión.
5. INSTALACIONES, GESTIÓN Y CONTROLES OPERATIVOS.
5.1 Controles Físicos.
5.1.1 **Ubicación y construcción del sitio**.
5.1.2 Acceso físico.
5.1.3 Energía y aire acondicionado.
5.1.4 Exposición al agua.
5.1.5 Prevención y protección contra incendios.
5.1.6 Almacenamiento de medios.
5.1.7 Eliminación de residuos
5.1.8 Copia de seguridad fuera de sitio.
5.2 Controles de Procedimiento.
5.2.1 Roles de confianza.
5.2.2 Número de personas necesarias por tarea.
5.2.3 Identificación y autenticación de cada rol.
5.2.4 Roles que requieren segregación de funciones.
5.3 Controles de personal.
5.3.1 Cualificaciones, experiencia y requisitos de habilitación
5.3.2 Procedimiento de verificación de antecedentes.
5.3.3 Requisitos de formación.
5.3.4 Requisitos y frecuencia de actualización de formación.
5.3.5 Frecuencia y secuencia de rotación de tareas.
5.3.6 Sanciones por acciones no autorizadas.
5.3.7 Requisitos para contratación de terceros.
5.3.8 **Documentación suministrada al personal.**
5.4 Procedimientos de Registro de Auditoría.
5.4.1 Tipo de eventos registrados.
5.4.2 Frecuencia de procesamiento de Logs.
5.4.3 Periodo de retención de los registros de auditoría.
5.4.4 Protección de los registros de auditoría.
5.4.5 Procedimiento de copia de seguridad de los registros de auditoría.

5.4.6 Sistema de recopilación de auditorías (interna o externa)
5.4.7 Notificación al sujeto causante del incidente de seguridad
5.4.8 Evaluaciones de vulnerabilidad.
5.5 Archivo de Registros.
5.5.1 Tipos de registros archivados.
5.5.2 Periodo de retención para archivo
5.5.3 Protección de archivo
5.5.4 Procedimientos de copia de seguridad de archivos
5.5.5 Requisitos para el sellado de tiempo de los registros.
5.5.6 Sistema de recolección de archivos (interna o externa).
5.5.7 Procedimientos para obtener y verificar información de archivo.
5.6 Cambio de Llaves.
5.7 Compromiso y Recuperación ante Desastres.
5.7.1 Procedimientos de gestión de incidentes y compromisos
5.7.2 Procedimiento en caso de daño de los recursos informáticos, el software y/o los datos.
5.7.3 Procedimientos de compromiso de la clave privada de la entidad.
5.7.4 Capacidad de recuperación en caso de desastre.
5.8 Cese de la CA o la RA.
6. CONTROLES TÉCNICOS DE SEGURIDAD.
6.1 Generación e Instalación de Pares de Claves.
6.1.1 Generación de pares de claves
6.1.2 Entrega de la clave privada al suscriptor.
6.1.3 Entrega de la clave pública al emisor del certificado.
6.1.4 Entrega de la clave pública de la AC a las partes que confían.
6.1.5 Tamaño de las Claves.
6.1.6 Generación de parámetros de clave pública y control de calidad.
6.1.7 Fines de uso de la clave (según el campo de uso de la clave X.509 v3).
6.2 Protección de clave privada y controles de ingeniería de módulos criptográficos.
6.2.1 Estándares y controles de los módulos criptográficos.
6.2.2 Control multipersona (m de n) de la clave privada.
6.2.3 Custodia de la clave privada.
6.2.4 Copia de respaldo de la clave privada.
6.2.5 Archivo de la clave privada.
6.2.6 Transferencia de clave privada o desde un módulo criptográfico.
6.2.7 Método de activación de la clave privada.
6.2.8 Método de desactivación de la clave privada.
6.2.9 Método de destrucción de la clave privada.
6.2.10 Clasificación del módulo criptográfico.
6.3 Otros aspectos de la gestión de pares de claves.
6.3.1 Archivo de la clave pública.
6.3.2 Periodos operativos de los certificados y periodos de uso de los pares de claves.
6.4 Datos de Activación.
6.4.1 Generación e instalación de los datos de activación.
6.4.2 Protección de los datos de activación.
6.4.3 Otros aspectos de los datos de activación.
6.5 Controles de Seguridad Informática.
6.5.1 Requisitos técnicos específicos de seguridad informática.
6.5.2 Clasificación de la seguridad informática.
6.6 Controles Técnicos del Ciclo de Vida.
6.6.1 Controles de desarrollo del sistema.
6.6.2 Controles de gestión de seguridad.
6.6.3 Controles de seguridad del ciclo de vida.
6.7 Controles de Seguridad de la Red.
Elementos del Plan de Continuidad
6.8 Sellado de Tiempo.
7. PERFILES DE CERTIFICADO, CRL Y OCSP.
7.1 Perfil del Certificado.
7.1.1 Números de versión.
7.1.2 Extensiones del certificado.
7.1.3 Identificadores de objetos algorítmicos.
7.1.4 Formas de nombres.
7.1.5 Restricciones de nombres.
7.1.6 Identificador del objeto de la Política de Certificación.
7.1.7 Uso de la extensión “Policy Constrains”.
7.1.8 Sintaxis y semántica de los calificadores de políticas
7.1.9 Tratamiento semántico para la extensión de políticas de certificados críticos.
7.2 Perfil de CRL.
7.2.1 Número(s) de versión
7.2.2 CRL y extensiones de entrada CRL
7.3 Perfil OCSP.
7.3.1 Número(s) de versión
7.3.2 Extensiones OCSP
8. AUDITORIA DE CUMPLIMIENTO Y OTRAS EVALUACIONES.
8.1 Frecuencia o Circunstancias de la Evaluación.
8.2 Identidad y cualificaciones del evaluador.
8.3 Relación del evaluador con la entidad evaluada.
8.4 Temas cubiertos por la evaluación.
8.5 Acciones tomadas como resultado de la deficiencia.
8.6 Comunicación de Resultados.
9. OTROS ASUNTOS COMERCIALES Y LEGALES.
9.1 Honorarios.
9.1.1 Tasas de emisión de certificados
Tarifas de emisión o renovación de certificados.
9.1.2 Tasas de acceso a certificados
9.1.3 Tasas de acceso a información sobre revocación o estado
9.1.4 Tasas por otros servicios
9.1.5 Políticas de Reembolso
9.2 Responsabilidad Financiera.
9.2.1 Cobertura del seguro.
9.2.2 Otros activos.
9.2.3 Cobertura de seguro o garantía para entidades finales
9.3 Confidencialidad de la Información Comercial.
9.3.1 Alcance de la información confidencial.
9.3.2 Información no confidencial.
9.3.3 Responsabilidad de proteger la información confidencial.
9.4 Privacidad de la Información Personal.
9.4.1 Plan de Privacidad.

9.4.2 Información tratada como privada.
9.4.3 Información que no se considera privada.
9.4.4 Responsabilidad de proteger la información privada.
9.4.5 Aviso y consentimiento para utilizar información privada.
9.4.6 Divulgación en virtud de un procedimiento judicial o administrativo.
9.4.7 Otras circunstancias de divulgación de información.
9.5 Derechos de Propiedad Intelectual.
9.6 Representaciones y Garantías.
9.6.1 Declaraciones y garantías de la AC
9.6.2 Declaraciones y garantías de la AR
9.6.3 Declaraciones y garantías del suscriptor
9.6.4 Declaraciones y garantías de la parte que confía
9.6.5 Declaraciones y garantías de otros participantes
9.7 Renuncias de Garantías.
9.8 Límites de Responsabilidad.
9.9 Indemnizaciones.
9.10 Duración y Terminación.
9.10.1 Duración.
9.10.2 Terminación.
9.10.3 Efecto de terminación, notificación y comunicación.
9.10.4 Procedimiento de Cambio en la DPC y PC.
9.11 Notificaciones y comunicaciones individuales a los participantes.
9.11.1 Obligaciones de la ECI **Letmi Ecuador S.A**.
9.11.2 Obligaciones de la AR.
9.11.3 Obligaciones (Deberes y Derechos) del suscriptor y/o Responsable.
9.11.4 Obligaciones de los Terceros que confían.
9.11.5 Obligaciones de la Entidad (Cliente).
9.11.6 Obligaciones de otros participantes de la ECI.
9.12 Enmiendas.
9.12.1 Procedimiento para enmienda.
9.12.2 Mecanismo y plazo de notificación.
9.12.3 Circunstancias en las que debe modificarse un OID.
9.12.4 Notificación al suscriptor o responsable de la emisión de un nuevo certificado.
9.12.5 Forma en la que se acepta la modificación de un certificado.
9.12.6 Publicación del certificado modificado por la ECI.
9.12.7 Notificación de la emisión de un certificado por la ECI a otras entidades.
9.13 Disposiciones sobre resolución de disputas.
9.14 Legislación aplicable.
9.15 Cumplimiento de la legislación aplicable.
9.16 Disposiciones varias.
9.16.1 Acuerdo completo
9.16.2 Cesión
9.16.3 Divisibilidad
9.16.4 Ejecución (honorarios de abogados y renuncia de derechos)
9.16.5 Fuerza mayor
9.17 Otras Disposiciones.
CAMBIOS QUE AFECTEN LOS SERVICIOS DE CERTIFICACIÓN DIGITAL.
DESCRIPCIÓN DE PRODUCTOS Y SERVICIOS
POLÍTICAS DE CERTIFICACIÓN.
ANEXO 1 DPC MATRIZ PERFIL TÉCNICO CERTIFICADOS DIGITALES.
ANEXO 2 DPC MODELOS Y MINUTAS DE LOS DOCUMENTOS DE TÉRMINOS Y CONDICIONES.
Letmi Ecuador S.A

1. INTRODUCCIÓN.

1.1 Descripción General

La Declaración de Prácticas de Certificación (en adelante DPC)- Global Certification Authority Root Letmi Ecuador S.A es un documento elaborado por **Letmi Ecuador S.A** que actuando como una Entidad de Certificación Digital, contiene las normas, declaraciones sobre las políticas y procedimientos que la **Entidad de Certificación de Información en adelante ECI Letmi Ecuador S.A** como **Prestador de Servicios de Certificación Digital (PSC)** aplica como lineamiento para prestar los servicios de certificación digital de acuerdo a lo establecido en la Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos, vigente. Reglamento a la Ley de Comercio Electrónico, vigente. ARCOTEL es la Agencia de Regulación y Control de las Telecomunicaciones que acredita ante el Estado Ecuatoriano a **Letmi Ecuador S.A** y los reglamentos que los modifiquen o complementen, en el territorio de Ecuador.

La DPC está conforme con los siguientes lineamientos:

1. La DPC está organizada bajo la estructura definida en el documento RFC 3647 Internet x.509 Public Key Infraestructure Certificate Policy and Certification Practice Framework de grupo de trabajo IETF - The Internet Engineering Task Force, (que sustituye a la RFC2527) http://www.ietf.org/rfc/rfc3647.txt?number=3647.
2. ETSI EN 319 411-1 V1.4.1 (2023-10).
3. RFC 6960 X.509 Internet Public Key Infrastructure En línea Certificate Status Protocol – OCSP.

Adicionalmente a las prácticas establecidas en esta DPC, cada tipo de certificado emitido por **Letmi Ecuador S.A** - se rige por los requisitos particulares establecidos en la correspondiente Política de Certificados (PC). Estas PC se encuentran publicadas en la misma página web de **Letmi Ecuador S.A.,** así como el presente documento. El presente documento es de carácter público y se encuentra dirigido a todas las personas naturales y jurídicas, solicitantes, suscriptores, terceros que confían y público en general.

La actualización y/o modificación de la DPC, se realizará a través del procedimiento establecido por **Letmi Ecuador S.A.** de información documentada, cualquier cambio o adecuación sobre el documento deberá ser revisado, analizado y aprobado por el Apoderado.

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

DATOS DE LETMI ECUADOR S.A:

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 Número: 126 Intersección: AV. AMAZONAS Edificio: BELMONTE Número de oficina: 5 Número de piso: 3
Ciudad / País:	Quito - Ecuador
Teléfono:	+59 (3) 99 351 6466
Correo electrónico:	info@letmi.app

Página Web:	https://letmi.app/

1.2 Nombre e identificación del documento.

La **DPC** para **ECI Letmi Ecuador S.A** se denominará “Declaración de Prácticas de Certificación (DPC)” La versión cambia de acuerdo con las modificaciones sobre el mismo documento.

Siguiendo los estándares de certificación digital, **Letmi Ecuador S.A** utiliza Identificadores de Objetos (OID) definidos en el estándar ITU-T Rec. X.660 (2004) | ISO/IEC 9834-1:2005 “Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs”.

Cada política de certificación está identificada por un único identificador de objeto (OID) que además incluye el número de versión.

La jerarquía de OIDs fue establecida por ECI **Letmi Ecuador S.A** a partir de la raíz 1.3.6.1.4.1.62566.1.1.5 definida por la IANA y está conforme a los siguientes parámetros:

JERARQUIA OID	DESCRIPCION	NOMBRE
1	Formato ISO	No varia
3	Organización	No varia
6	Publico	No varia
1	Internet	No varia
4.1 (62566)	Identificación de la organización	No varia, definida por la IANA
1	Tipo de documento	Cambia dependiendo si son políticas, procedimientos, manuales entre otros
1	Número del documento	Este es el número asignado al documento entre su grupo
5	Versión del documento	Se modifica de acuerdo con cada versión del documento

Nombre de la DPC	**Declaración de Prácticas de Certificación**
Número de versión	5
Grupo de Trabajo	Comité de Gerencia
Estado de la DPC	Vigente
Fecha de publicación en el repositorio	21/04/2026
Fecha de creación del documento	27/01/2025
Fecha de inicio de vigencia	21/04/2026
OID (Object Identifier) - IANA único asignado	1.3.6.1.4.1.62566.1.1.5
Ubicación de la DPC (Versión vigente)	https://letmi.app/documentos/Marco_regulatorio/DPC/Declaracion_de_Practicas_de_Certificacion_V5.pdf
Elaboró	Coordinador de Operaciones
Revisó	Sistema Integrado de Gestión
Aprobó	Apoderado
Fecha de Aprobación Interna	21/04/2026

Historial de Cambios

Versión	Fecha	Cambio/Modificación
1	27/01/2025	Documento inicial
2	03/09/2025	Se ajusta número de contacto de la ECI
3	16/02/2026	Se ajustan los siguientes numerales: • 1.3.1 Autoridad de Certificación (AC): Cambio del datacenter y datos de ubicación del mismo. • 7.1 Perfil del Certificado: En la tabla “Datos capturados en la solicitud” se adicionan las columnas para los tipos de certificado Sello Electrónico -SE (En Archivo), Persona Natural - PN (En Archivo) y Representante Legal - RL (En Archivo). • Políticas de certificación: Ajuste en el nombre de las políticas de acuerdo a la adición de nuevo formato en archivo. • Se agregan campos de firma de elaboró, revisó y aprobó al final del documento.
4	27/03/2026	Se ajustan los siguientes numerales: • 1. 2 Nombre e identificación del documento: Se incluyeron ajustes tales como el nombre exacto de la DPC, el OID único asignado, el número de versión, el historial de cambios, la fecha de aprobación interna, la fecha de publicación en el repositorio, el estado del documento (vigente) y la URL actualizada para el acceso público a la versión vigente del documento. •2.4 Control de Acceso: Se incorpora una descripción detallada de los controles implementados por la entidad. En este sentido, se incluyeron de manera explícita los mecanismos de control de acceso. Asimismo, se integraron los mecanismos orientados a garantizar la integridad de la información, junto con la definición de compromisos formales relacionados con la revisión periódica y auditoría de dichos controles, con el fin de asegurar su adecuada implementación y efectividad. • 3. Identificación y Autenticación: Se amplia la descripción detallada de los procesos aplicables según el tipo de certificado emitido. Asimismo, se incluyeron los mecanismos de identificación y autenticación correspondientes, junto con la especificación del mecanismo criptográfico utilizado en cada caso. • 4.5 Uso de pares de claves y certificados: Se incluyeron los tamaños de clave utilizados, así como los algoritmos hash aplicables. Adicionalmente, se definieron las condiciones relacionadas con la generación y almacenamiento de la clave privada, estableciendo el uso de dispositivos seguros, como módulos de seguridad hardware (HSM). • 8.2 Identidad y cualificaciones del evaluador: Se actualizó el numeral incorporando la especificación de que la entidad evaluadora o de inspección debe contar

		con la debida acreditación otorgada por el organismo nacional de acreditación competente, así como su reconocimiento por parte de la autoridad de control correspondiente. • 8.6 Comunicación de resultados: Se ajusta el numeral incorporando de manera expresa el plazo de quince (15) días hábiles para el envío correspondiente, contado a partir de la finalización del proceso, en cumplimiento de la normativa técnica vigente de ARCOTEL.. • 9.1 Tarifas: Se incorpora un detalle completo, desglosado y de acceso público de los costos asociados a los servicios ofertados, incluyendo la emisión, renovación, revocación, consulta y demás servicios relacionados incluyendo la estructura de precios correspondiente y las condiciones de pago aplicables. • 9.4 Privacidad de la Información personal: Se actualizó la sección 9.4 incorporando de manera expresa los derechos del titular de los datos personales, incluyendo acceso, rectificación y supresión, conforme a la terminología establecida en la normativa aplicable la Ley Orgánica de Protección de Datos Personales (LOPDP). Asimismo, se incluyeron los plazos de retención de la información personal una vez expirado el certificado. • 9.8 Limitaciones de Responsabilidad: Se adicionan las condiciones correspondientes a la garantía contratada por Letmi Ecuador S.A detallando adicionalmente el monto por el cual se contrató la misma y las condiciones de reclamación.
5	21/04/2026	• Se modifica diseño del documento. • Se amplía el servicio de certificación mediante la incorporación, en el presente documento, de los certificados para miembros de empresa o empleados en relación de dependencia, tanto en formato archivo como en dispositivo seguro de creación de firma (DSCF). • Subsanación de las observaciones emitidas por ARCOTEL. mediante el Oficio Nro. ARCOTEL-CTDS-2026-0453-OF.

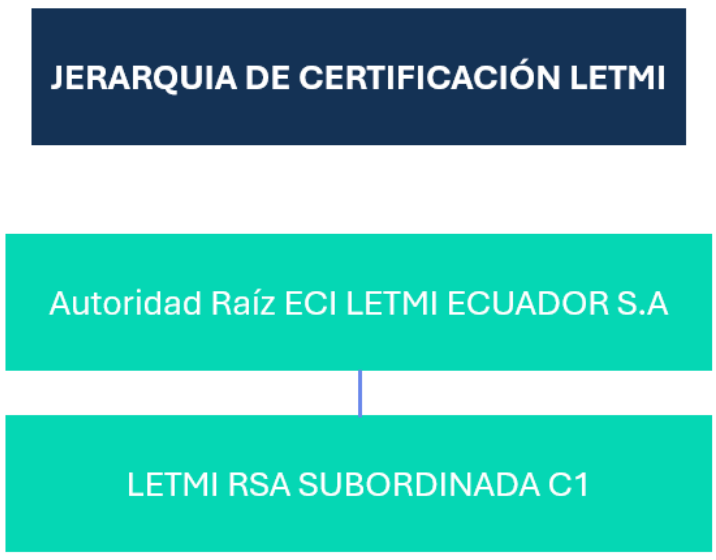
1.3 Participantes PKI.

1.3.1 Autoridad de Certificación (AC).

La AC realiza tareas relacionadas con la gestión del ciclo de vida, emisión, renovación y distribución de los certificados de firma digital. La AC proporciona el estado de los certificados de firma digital por medio de la lista de revocación de certificados (CRL) y por el protocolo de estado de certificados en línea (OCSP). Garantiza la disponibilidad de todos los servicios relacionados con la gestión de los certificados de firma digital.

Jerarquía de las AC´s.

La jerarquía de certificación de **Letmi Ecuador S.A** está compuesta por las siguientes Autoridades Certificadoras (AC):



ECI LETMI ECUADOR S.A AC tiene dos datacenter, el datacenter (Activo) con Sencinet Latam Colombia S.A ICD Nimbus, ubicado en la Carrera 106 No. 15A25 Manzana 4 Lote 38 Zona Franca, Bogotá, Colombia y el Datacenter (Activo) con Claro se encuentra ubicado en la Autopista Medellin Km 7.5 Celta Trade Park – Datacenter Triara, Cota, Cundinamarca, Colombia.

1.3.2 Autoridad de Registro (AR).

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 información y/o documentación del suscriptor o responsable de los servicios de certificados de firma digital, en la AR 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 DPC, la figura de AR 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 (AR).

1.3.3 Suscriptor

El suscriptor es la persona natural o jurídica a la cual se emiten o activan los servicios de certificación digital y por tanto actúa como suscriptor y/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 suscriptor será diferente dependiendo de los servicios prestados por la ECI **Letmi Ecuador S.A** conforme lo establecido en las Políticas de Certificados de Certificación Digital.

1.3.4 Partes de confianza.

La persona natural el responsable al cual se le 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.

Los terceros que confían deben actuar con base en los principios de buena fe y lealtad, absteniéndose de realizar conductas fraudulentas o negligentes cuyo fin sea repudiar los procesos de identificación o firma digital, sello de tiempo, o cualquier tipo de manipulación de los certificados electrónicos.

1.3.5 Otros participantes.

Proveedores de servicios.

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

Entidades de Certificación Digital 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 digital 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.

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 DPC y sus políticas; 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 suscriptores, responsables y terceros.

Teléfono: +59 (3) 99 351 6466

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 el área de Servicio al Cliente es la 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 suscriptor, responsable y/o parte interesada.

La ECI atenderá y resolverá en el término máximo de quince (15) días las solicitudes y reclamos presentadas por los usuarios, así como comprobará la veracidad, autenticidad, exactitud y validez de la información suministrada por los solicitantes del servicio, respecto de su identidad y otros datos relevantes, previo a la provisión efectiva de los servicios requeridos

1.4 Uso del certificado.

1.4.1 Uso permitido de los certificados

Los usos adecuados de los Certificados emitidos por ECI **Letmi Ecuador S.A** vienen especificados en las Políticas de Certificado para Certificados Digitales.

Los Certificados emitidos bajo esta DPC pueden ser utilizados con los siguientes propósitos:

- **Identificación del suscriptor:** El suscriptor del Certificado Digital puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el Certificado Digital.
- **Integridad:** La utilización del Certificado Digital para aplicar firmas digitales garantiza que el documento firmado es integro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el suscriptor. Se certifica que el mensaje recibido por el Receptor o Destino que confía es el mismo que fue emitido por el suscriptor.
- **No repudio:** Con el uso de este Certificado Digital también se garantiza que la persona que firma digitalmente el documento no puede repudiarlo, es decir, el suscriptor que ha firmado no puede negar la autoría o la integridad de este.

La clave pública contenida en un Certificado Digital puede utilizarse para cifrar mensajes de datos, de tal manera que únicamente el poseedor de la clave privada puede descifrar dicho mensaje de datos y acceder a la información. Si la clave privada utilizada para descifrar se pierde o se destruye, la información que haya sido cifrada no podrá ser descifrada. El suscriptor, responsables y los terceros de buena fe, reconocen y aceptan los riesgos que representa hacer uso de los certificados digitales para realizar procesos de cifrado y en especial la utilización de las claves para cifrar mensajes de datos es de exclusiva responsabilidad del suscriptor o responsable en caso de materializar una pérdida o destrucción de la clave.

La ECI **Letmi Ecuador S.A** no asume ninguna responsabilidad por el uso de los certificados digitales para procesos de cifrado.

Cualquier otro uso que no esté descrito en esta DPC se considerará una violación a esta DPC y constituirá una causal de revocación inmediata del servicio de certificación digital y terminación del contrato con el suscriptor y/o responsable, sin perjuicio de las acciones penales o civiles a las que haya lugar por parte de la ECI **Letmi Ecuador S.A**.

El suscriptor podrá hacer uso del certificado según lo establecido a continuación:

- Autenticación
- Firma digital de documentos
- Correos electrónicos
- Cifrado de transacciones y archivos
- Otras aplicaciones de firma digital, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

1.4.1.1 Uso permitido del certificado de Persona Natural en DSCF y en archivo

El Certificado de Persona Natural emitido bajo el formato DSCF y en archivo debe ser utilizado exclusivamente por su titular para fines de identificación y firma digital en el marco de las transacciones electrónicas autorizadas. Su uso es personal, intransferible y está sujeto al cumplimiento de las políticas, prácticas de certificación y normativa aplicable. El titular es responsable de la custodia de su clave privada y de evitar cualquier uso indebido, debiendo notificar de manera inmediata a la entidad de certificación ante cualquier sospecha de compromiso, pérdida o uso no autorizado, a fin de proceder con la revocación correspondiente y mitigar posibles riesgos.

1.4.1.2 Uso permitido del certificado de Sello electrónico en DSCF y en archivo

El Certificado de Sello Electrónico emitido bajo el formato DSCF y en archivo debe ser utilizado exclusivamente por la persona jurídica titular para garantizar la autenticidad e integridad de los documentos electrónicos generados en el ejercicio de sus funciones. Su uso está restringido a los fines definidos en la política y prácticas de certificación, y no implica representación de voluntad individual, sino la identificación de la entidad. La organización es responsable de la adecuada administración, custodia y control de los dispositivos y claves asociados, así como de prevenir su uso indebido, debiendo notificar de manera inmediata a la entidad de certificación ante cualquier sospecha de compromiso, pérdida o uso no autorizado, con el fin de proceder a su revocación y mitigar posibles riesgos.

1.4.1.3 Uso permitido del certificado de Representante legal en DSCF y en archivo

El Certificado de Representante Legal emitido bajo el formato DSCF y en archivo debe ser utilizado exclusivamente por la persona natural que ostenta dicha calidad, con el fin de actuar en nombre y representación de la persona jurídica en las transacciones electrónicas autorizadas. Su uso implica la manifestación de voluntad de la entidad, dentro de las facultades otorgadas al titular, y está sujeto al cumplimiento de las políticas y prácticas de certificación, así como de la normativa aplicable. El titular es responsable de la custodia de su clave privada y de evitar cualquier uso indebido, debiendo notificar de manera inmediata a la entidad de certificación ante cualquier sospecha de compromiso, pérdida o uso no autorizado, a fin de proceder con la revocación correspondiente y mitigar posibles riesgos.

1.4.1.4 Uso permitido del certificado de Miembro empresa o en relación de dependencia en DSCF y en archivo

El Certificado de Miembro de Empresa o en Relación de Dependencia, emitido bajo el formato DSCF y en archivo, debe ser utilizado exclusivamente por la persona natural titular del mismo, con el fin de realizar transacciones electrónicas en el marco de sus funciones y en virtud de su vinculación laboral o contractual con la persona jurídica. Su uso implica la manifestación de voluntad del titular dentro de las facultades propias de su cargo, sin que ello represente, por sí mismo, la voluntad de la entidad ni el otorgamiento de facultades adicionales. El uso del certificado se encuentra sujeto al cumplimiento de las políticas y prácticas de certificación, así como de la normativa aplicable. El titular es responsable de la custodia de su clave privada y de prevenir cualquier uso indebido, debiendo notificar de manera inmediata a la entidad de certificación ante cualquier sospecha de compromiso, pérdida o uso no autorizado, con el fin de proceder a su revocación y mitigar posibles riesgos.

1.4.2 Uso prohibido de los certificados

Los certificados sólo podrán ser empleados para los usos para los que hayan sido emitidos y especificados en esta DPC y concretamente en las Políticas De Certificado para Certificados Digitales.

Se consideran usos indebidos aquellos que no están definidos en esta DPC y en consecuencia para efectos legales, ECI **Letmi Ecuador S.A** queda eximida de toda responsabilidad por el empleo de los certificados en operaciones que estén fuera de los límites y condiciones establecidas para el uso de Certificados Digitales según esta DPC, dentro de los que se incluyen, pero sin limitarse a los siguientes usos prohibidos:

- Fines u operaciones ilícitas bajo cualquier régimen legal del mundo.
- Cualquier práctica contraria a la legislación Ecuatoriana.
- Cualquier práctica contraria a los convenios internacionales suscritos por el estado Ecuatoriano.
- Cualquier práctica contraria a las normas supranacionales.
- Cualquier práctica contraria a las buenas costumbres y prácticas comerciales.
- Cualquier uso en sistemas cuyo fallo pueda ocasionar:
  - Muerte.
  - Lesiones a personas.
  - Perjuicios al medio ambiente.
- Como sistema de control para actividades de alto riesgo como son:
  - Sistemas de navegación marítimo.
  - Sistemas de navegación de transporte terrestre.
  - Sistemas de navegación aéreo.
  - Sistemas de control de tráfico aéreo.
  - Sistemas de control de armas.

1.4.2.1 Uso prohibido del certificado de Persona Natural en DSCF y en archivo

El Certificado de Persona Natural no debe ser utilizado por terceros distintos a su titular, ni para actuar en representación de una persona jurídica o de otro individuo. Asimismo, está prohibido su uso en actividades ilícitas, en transacciones no autorizadas o que excedan los fines definidos en la DPC, así como en sistemas o contextos donde no se garantice la seguridad de la clave privada. No debe emplearse cuando exista sospecha de compromiso, pérdida o uso indebido del certificado.

1.4.2.2 Uso prohibido del certificado de Sello Electrónico en DSCF y en archivo

El Certificado de Sello Electrónico no debe ser utilizado para manifestar voluntad o consentimiento en nombre de una persona natural, ni para firmar documentos que impliquen decisiones individuales. Está prohibido su uso fuera de los fines de autenticación e integridad de documentos electrónicos definidos en la DPC, así como en actividades ilícitas o no autorizadas. Tampoco debe utilizarse en caso de compromiso, pérdida de control o acceso no autorizado a los dispositivos o claves asociadas.

1.4.2.3 Uso prohibido del certificado de Representante Legal en DSCF y en archivo

El Certificado de Representante Legal no debe ser utilizado por personas distintas a su titular, ni para actuar fuera de las facultades otorgadas por la persona jurídica que representa. Se prohíbe su uso en actividades ilícitas, en transacciones no autorizadas o que excedan los fines establecidos en la DPC. Asimismo, no debe emplearse en caso de compromiso, pérdida o uso indebido de la clave privada, ni cuando el titular haya cesado en sus funciones como representante legal.

1.4.2.4 Uso prohibido del certificado de Miembro empresa o en relación de dependencia en DSCF y en archivo

El Certificado de Miembro de Empresa o en Relación de Dependencia no debe ser utilizado por personas distintas a su titular, ni para la realización de actuaciones que excedan las funciones propias del cargo o la vinculación que este mantiene con la persona jurídica. Se prohíbe su uso en actividades ilícitas, en transacciones no autorizadas o que no correspondan al ámbito de sus funciones, así como en aquellas que contravengan los fines establecidos en la DPC. Asimismo, no debe emplearse en caso de compromiso, pérdida o uso indebido de la clave privada, ni cuando el titular haya cesado en su vinculación laboral o contractual con la entidad correspondiente.

1.5 Administración de políticas.

1.5.1 Organización que administra el documento.

La DPC y las políticas de certificación son responsabilidad y propiedad de la ECI **Letmi Ecuador S.A.** y por tanto actúa como su administradora.

DATOS DE LA ECI LETMI ECUADOR S.A. ENTIDAD ADMINISTRADORA DEL DOCUMENTO:

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 Número: 126 Intersección: AV. AMAZONAS Edificio: BELMONTE Número de oficina: 5 Número de piso: 3
Ciudad / País:	Quito - Ecuador
Teléfono:	+59 (3) 99 351 6466
Correo electrónico:	info@letmi.app
Página Web:	https://letmi.app/
Responsable	Lilianne Martinez Ledea

Cargo	Apoderado

1.5.2 Contacto (Responsable de la ECI):

Nombre: Lilianne Martinez Ledea

Cargo: Apoderado

Dirección: Calle Corea #126 Av Amazonas Edificio Belmonte Oficina 5 Piso 5

Domicilio: Quito, Ecuador.

Teléfono: +59 (3) 99 351 6466

Correo electrónico: info@letmi.app

Correo electrónico comercial: comercia@letmi.app

Horarios de atención: Lunes a viernes de 8:30 am a 5:30 pm

Página web: https://letmi.app/

Plazos de respuestas para consultas específicas sobre la DPC: 15 días hábiles.

1.5.3 Persona que determina la idoneidad de la DPC para la póliza.

La persona que determina la idoneidad de la DPC es el Responsable de la Entidad de Certificación de **Letmi Ecuador S.A.**

1.5.4 Procedimientos de aprobación de la DPC.

El Representante Legal es el responsable de **Letmi Ecuador S.A** encargado de la revisión, aprobación y autorización de la publicación de la DPC en la página Web https://letmi.app/

1.6 Definiciones y acrónimos.

Definiciones.

Los siguientes términos son de uso común y requerido para el entendimiento de la presente DPC:

Autoridad de Certificación (AC): 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 (AR): 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.

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: Dispositivo criptográfico seguro, certificados remotos o en nube (HSM) y certificados en tarjeta criptográfica.

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 tiempos 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 suscriptor, 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 suscriptor, 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 suscriptor 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.

Pseudonimo: Oculta con un nombre falso el suyo verdadero.

Pseudoanonimo: Utiliza un nombre falso de manera intencional

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.

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

Tercero de buena fe: Persona o entidad diferente del suscriptor 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.

Acrónimos.

AC: Autoridad de Certificación

CA Sub: Autoridad de Certificación Subordinada

AR: Autoridad de Registro

PC: Política de Certificación (Certificate Policy)

DPC: Declaración de Prácticas de Certificación (Certificate Practice Statement)

DSCF: Dispositivo Seguro de Creación de Firma

ECI: Entidad de Certificación de Información

CRL: Certificate Revocation List

CSP: Certification Service Provider

DNS: Domain Name System

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.

HSM: Módulo de seguridad criptográfico (Hardware Security Module)

IEC: International Electrotechnical Commission

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

IP: Internet Protocol

ISO: International Organization for Standardization

LDAP: Lightweight Directory Access Protocol

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

RNEC: Registraduría Nacional del Estado Civil

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

URL: Uniform Resource Locator

VA: Autoridad de validación (Validation Authority)

Estándares y Organismos de estandarización.

CEN: Comité Europeo de Normalización

CWA: CEN Workshop Agreement

ETSI: European Telecommunications Standard Inst

FIPS: Federal Information Processing Standard

IETF: Internet Engineer Task Force

PKIX: Grupo de trabajo del IETF sobre PKI

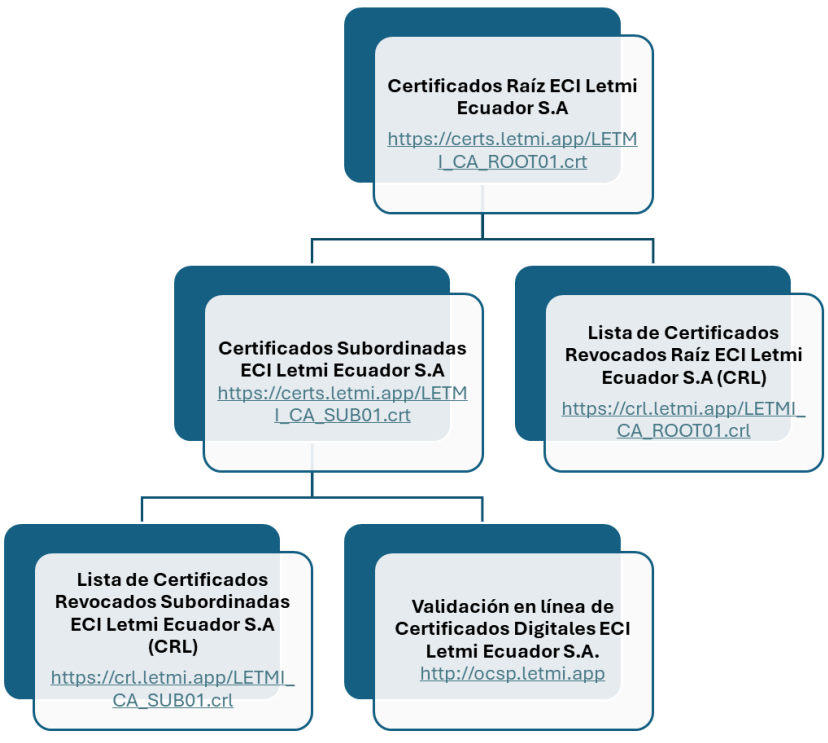
PKCS: Public Key Cryptography Standards

RFC: Request For Comments

2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO.

Los servicios de consulta y acceso a los repositorios de la DPC se proporcionan mediante las direcciones electrónicas oficialmente habilitadas para la verificación de certificados digitales. En caso de presentarse cambios en estas direcciones, se informará de manera oportuna a las partes interesadas. Las direcciones IP asociadas a dichos servicios pueden variar y no son fijas, por lo que su modificación podrá realizarse sin notificación previa, garantizando en todo caso la continuidad del servicio.

2.1 Repositorios.



- **Declaración de Practicas de Certificación**

https://letmi.app/documentos/Marco_regulatorio/DPC/Declaracion_de_Practicas_de_Certificacion_V5.pdf

- **Políticas de certificado para servicio de certificados digitales Persona Natural en DSCF y en archivo**

https://letmi.app/documentos/Marco_regulatorio/politicas/Politicas_de_Certificado_para_Certificados_Digitales_Persona_Natural_DSCF_y_en_Archivo_V4.pdf

- **Políticas de certificado para servicio de certificados digitales Sello Electrónico en DSCF y en archivo**

https://letmi.app/documentos/Marco_regulatorio/politicas/Politicas_de_Certificado_para_Certificados_Digitales_Sello_Electronico_DSCF_y_en_Archivo_V4.pdf

- **Políticas de certificado para servicio de certificados digitales Representante Legal en DSCF y en archivo**

https://letmi.app/documentos/Marco_regulatorio/politicas/Politicas_de_Certificado_para_Certificados_Digitales_Representante_Legal_DSCF_y_en_Archivo_V4.pdf

- **Políticas de Certificado para Servicio de Certificados Digitales Miembro Empresa o en Relación de Dependencia en DSCF y en Archivo**

https://letmi.app/documentos/Marco_regulatorio/politicas/Politicas_de_Certificado_para_Certificados_Digitales_Miembro_Empresa_o_en_Relacion_de_Dependencia_en_DSC

- **Certificados Raíz ECI Letmi Ecuador S.A**

https://certs.letmi.app/LETMI_CA_ROOT01.crt

- **Lista de Certificados Revocados Raíz ECI Letmi Ecuador S.A (CRL)**

https://crl.letmi.app/LETMI_CA_ROOT01.crl

- **Certificados Subordinadas ECI Letmi Ecuador S.A**

https://certs.letmi.app/LETMI_CA_SUB01.crt

- **Lista de Certificados Revocados Subordinadas ECI Letmi Ecuador S.A (CRL)**

https://crl.letmi.app/LETMI_CA_SUB01.crl

- **Validación en línea de Certificados Digitales ECI Letmi Ecuador S.A.**

http://ocsp.letmi.app

Nota: La validación en línea de certificados digitales mediante OCSP se debe realizar con una herramienta que implemente el protocolo OCSP y sea capaz de entender las respuestas generadas por el servicio, tal es el caso de OPENSSL.

Este repositorio de la ECI **Letmi Ecuador S.A.** no contiene ninguna información confidencial o privada.

Los repositorios de la ECI **Letmi Ecuador S.A.** están referenciados por la URL. Cualquier cambio en las URLs se notificará a todas entidades que puedan verse afectadas.

Las direcciones IP correspondientes a cada URL podrán ser múltiples y dinámicas, pudiendo ser modificadas sin previo aviso por ECI **Letmi Ecuador S.A**.

2.2 Publicación de información sobre certificación.

La Lista de Certificados Revocados publicada en la página web de **Letmi Ecuador S.A** está firmada digitalmente por la ECI **Letmi Ecuador S.A**.

La información del estado de los certificados digitales vigentes está disponible para consulta en la página Web y con el protocolo OCSP.

2.3 Plazo o frecuencia de la publicación.

Certificado Raíz

El certificado raíz se publicará y permanecerá en la página Web de ECI **Letmi Ecuador S.A** durante todo el tiempo en que se estén prestando servicios de certificación digital.

Certificado Subordinada

El certificado de la Subordinada se publicará y permanecerá en la página Web de ECI **Letmi Ecuador S.A** durante todo el tiempo en que se estén prestando servicios de certificación digital.

Lista de Certificados Revocados (CRL)

La ECI **Letmi Ecuador S.A** publicará en la página Web, la lista de certificados revocados en los eventos y con periodicidad como lo define el apartado *Frecuencia de emisión de las CRLs "*La ECI **Letmi Ecuador S.A** generará y publicará para sus entidades subordinadas una nueva CRL cada veinticuatro (24) horas en su repositorio con una disponibilidad de consulta en línea 7×24×365, 99.8% uptime por año; para las entidades Raíz el periodo de generación se establece en (1) año".

Declaración de Prácticas de Certificación (DPC) - Global Certification Authority Root

Con autorización del apoderado, la validación por parte de la firma de Auditoría, la emisión del informe de cumplimiento de la auditoria y finalmente con la acreditación expresa del ARCOTEL, se publicará la versión finalmente aprobada para la prestación del servicio de certificación digital y las publicaciones posteriores estarán sujetas a las modificaciones a que haya lugar con aprobación del apoderado. Los cambios generados en cada nueva versión serán informados a ARCOTEL y publicados en la página Web de ECI **Letmi Ecuador S.A** junto con la nueva versión. La Auditoria anual validará estos cambios y emitirá el informe de cumplimiento.

Validación en línea de Certificados Digitales

ECI **Letmi Ecuador S.A** publicará los certificados emitidos en un repositorio en formato X.509 los cuales podrán ser consultados en la dirección http://ocsp.letmi.app

La validación en línea de certificados digitales mediante OCSP se debe realizar con una herramienta que implemente el protocolo OCSP y sea capaz de entender las respuestas generadas por el servicio, tal es el caso de OPENSSL.

2.4 Controles de acceso a los repositorios.

La consulta a los repositorios disponibles en la página Web de **Letmi Ecuador S.A** antes mencionados, es de libre acceso al público en general. La integridad y disponibilidad de la información publicada es responsabilidad de ECI **Letmi Ecuador S.A** , que cuenta con los recursos y procedimientos necesarios para restringir el acceso a los repositorios con otros fines diferentes a la consulta.

Para el control de acceso a los repositorios se implementa gestión de roles y mecanismos de autenticación, tales como:

a. Segregación de roles, listas blancas, acceso por medio de certificados.Contraseñas seguras con características alfanumérico, mayúsculas, minúsculas y carácter especial

b. Usuarios basados en roles y privilegios de accesos

c. Bloqueo de sesión después de tres intentos fallidos

d. La información en tránsito se protege mediante el uso de SSL/TLS versión 1.3 con certificados digitales, garantizando su confidencialidad e integridad a través de algoritmos criptográficos como SHA-256.

e. La plataforma garantiza la protección en la capa de aplicación mediante un WAF de esta manera protegiéndose de ataques DDOS entre otros.

El ejercicio de auditoría de los controles de acceso a los repositorios se realiza periódicamente de acuerdo a lo establecido 8. Auditoría de cumplimiento y otras evaluaciones.

3. IDENTIFICACIÓN Y AUTENTICACIÓN.

3.1 Nombres.

3.1.1 Tipos de nombres.

Todos los certificados requieren un nombre distinguido (DN o distinguished name) conforme al estándar X.509. Adicionalmente, los DN de los certificados cualificados son coherentes con lo dispuesto en las normas: - ETSI EN 319 412-2 conocida como “Certificate profile for certificates issued to natural persons” RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", - RFC 3739 “Internet X.509 Public Key Infrastructure: Qualified Certificates Profile”.

Certificados Raíz de la ECI Letmi Ecuador S.A.

El DN del ‘issuer name’ del certificado Raíz de ECI **Letmi Ecuador S.A**, tienen las siguientes características:

C = EC
L = QUITO
O = LETMI ECUADOR S.A.
Organization Identifier= VATEC-1793221101001
OU = CA RSA ROOT (Certification Services)
CN = LETMI RSA ROOT C1

El DN del ‘subject name’ del certificado Raíz de ECI **Letmi Ecuador S.A**, tienen las siguientes características:
C = EC
L = QUITO
O = LETMI ECUADOR S.A.
Organization Identifier = VATEC-1793221101001
OU = CA RSA ROOT (Certification Services)
CN = LETMI RSA ROOT C1

Certificados de las Subordinadas ECI Letmi Ecuador S.A.

El DN del ‘issuer name’ del certificado Subordinado de ECI **Letmi Ecuador S.A**, tienen las siguientes características:

C = EC
L = QUITO
O = LETMI ECUADOR S.A.
Organization Identifier = VATEC-1793221101001
OU = CA RSA ROOT (Certification Services)
CN = LETMI RSA ROOT C1

El DN del ‘subject name’ del certificado Subordinado de ECI **Letmi Ecuador S.A**, tienen las siguientes características:

C = EC
L = QUITO
O = LETMI ECUADOR S.A.
Organization Identifier = VATEC-1793221101001
OU = CA RSA SUB (Certification Services)
CN = LETMI RSA SUB C1

El DN del ‘subject name’ del certificado Subordinado de ECI **Letmi Ecuador S.A**, por cada tipo de certificado tienen las siguientes características:

Certificado Persona Natural

SERIALNUMBER = Número de Identificación del solicitante IDC
C = País de domicilio del suscriptor
L = Localidad (Ciudad) domicilio del suscriptor
SN= Apellidos del Suscriptor (solicitante)
G= Nombres del suscriptor (solicitante)
CN= Nombres y apellidos del suscriptor

Certificado Sello Electrónico

C = País de domicilio del suscriptor
L = Localidad (Ciudad) domicilio del suscriptor
SERIALNUMBER = Número de Identificación del solicitante IDC
O = Nombre completo de la entidad (Empresa) con razón social
CN = Descripción uso certificado - Ejemplo (Recepción documentos ventanilla)
SN = Apellidos del Suscriptor (solicitante)
G = Nombres del suscriptor (Solicitante)

Certificado Representante Legal

SERIALNUMBER = Número de Identificación del solicitante IDC
C =País de domicilio del suscriptor
L = Localidad (Ciudad) domicilio del suscriptor
T =Nombre del título o puesto (cargo) del suscriptor ocupado en la empresa
O = Nombre completo de la entidad (Empresa) con razón social
SN = Apellidos del Suscriptor (solicitante)
G = Nombres del suscriptor (Solicitante)
CN = Nombres y apellidos del suscriptor

Certificado Miembro Empresa o Empleado con Relación de Dependencia

CN = Nombres y apellidos del suscriptor
SERIALNUMBER = Número de Identificación del solicitante IDC
G = Nombres del signatario
SN = Apellidos del signatario
T =Nombre del título o puesto (cargo) del signatario ocupado en la empresa
OU= Departamento o área al que pertenece el signatario
O = Nombre de la persona natural o la persona jurídica
L = Localidad (Ciudad) domicilio del signatario
C = País de domicilio del signatario

3.1.2 Necesidad de que los nombres tengan sentido.

Los nombres distintivos (DN) de los certificados emitidos por ECI **Letmi Ecuador S.A** son únicos y permiten establecer un vínculo entre la llave pública y el número de identificación del suscriptor. Debido a que una misma persona o entidad puede solicitar varios certificados a su nombre, estos se diferenciarán por el uso de un valor único en el campo DN.

3.1.3 Anonimato o seudonimato de los titulares de la firma.

No se podrán utilizar alias, sobrenombres, apodos, diminutivos, y/o semejantes en los campos de suscriptor o responsable ya que dentro del certificado debe figurar el verdadero nombre, razón social sigla o denominación del solicitante del certificado.

3.1.4 Reglas de interpretación de las distintas formas del nombre.

La regla utilizada para interpretar los nombres distintivos del emisor y de los suscriptores o responsables de certificados digitales que emite ECI **Letmi Ecuador S.A** es el estándar ISO/IEC 9595 (X.509) Distinguished Name (DN) y la sintaxis ASN.1.

3.1.5 Unicidad de los Nombres.

El DN de los certificados digitales emitidos es único para cada suscriptor.

3.1.6 Reconocimiento, autenticación y rol de las marcas registradas.

Reconocimiento, autenticación y papel de las marcas reconocidas ECI **Letmi Ecuador S.A** no está obligada a recopilar o solicitar evidencia en relación con la posesión o suscripción o responsabilidad de marcas registradas u otros signos distintivos antes de la emisión de los certificados digitales. Esta política se extiende al uso y empleo de nombres de dominio.

3.2 Validación inicial de identidad.

ECI **Letmi Ecuador S.A** deberá recibir solicitudes para certificar la identificación inequívoca de la identidad del suscriptor (persona natural o jurídica) la veracidad y autenticidad de la información a través de cualquier sistema de identificación, siempre y cuando subsista contrato, convenio, acuerdo, alianza, y/o cualquier medio de relación contractual y/o comercial, directa y/o indirectamente, entre otras.

La ECI **Letmi Ecuador S.A**, se reserva el derecho de declinar la aceptación de una solicitud o el mantenimiento de un contrato para la certificación cuando a su juicio existen razones que puedan poner en riesgo la credibilidad, valor comercial, idoneidad legal o moral de la ECI, así mismo la participación demostrada del solicitante en actividades ilegales, o temas similares relacionados con el mismo, será razón suficiente para rechazar la solicitud.

Los datos del solicitante: tipo de identificación, número de identificación, nombres, apellidos, RUC (**Registro Único de Contribuyentes)**, razón social (aplica para empresa) y correo electrónico son revisados y/o validados en conjunto con el formulario de solicitud, escritura de constitución, certificación de poderes y la información y/o documentación suministrada para cada tipo de certificado digital.

La ECI **Letmi Ecuador S.A**, se reserva el derecho de solicitar documentos adicionales, en original o copia; con el fin de verificar la identidad del solicitante, también puede eximir la presentación de cualquier documento cuando la identidad del solicitante haya sido suficientemente verificada por la ECI **Letmi Ecuador S.A** a través de otros medios.

La validación del solicitante descrita anteriormente se podrá verificar contra el registro civil, identificación y cedulación de Ecuador, dado que dicho ente es quien identifica los ciudadanos ecuatorianos y es el máximo ente de identificación en el país.

3.2.1 Método para demostrar la posesión de la clave privada.

En caso de que el certificado sea centralizado la generación del par de llaves se lleva a cabo en un dispositivo HSM de propiedad de la ECI **Letmi Ecuador S.A** y se le hace entrega al suscriptor y/o responsable de un conjunto de credenciales (usuario y contraseña) para el uso exclusivo de las mismas.

3.2.2 Autenticación de la identidad de la organización.

Para asegurar la identidad de una persona jurídica, la AR **Letmi Ecuador S.A** exige la presentación del documento oficial que acredite la existencia legal de la misma y su representante legal o apoderados quienes serán las únicas personas que puedan solicitar el certificado digital a nombre de dicha organización. Para el caso que la solicitud se realice por un tercero que confía, se debe entregar escaneada la constancia de delegación del proceso al apoderado. Los documentos se recibirán escaneados, preservando la legibilidad para el uso de la información.

No obstante, lo anterior, ECI **Letmi Ecuador S.A**, se reserva el derecho de emisión de certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial o idoneidad legal o moral de la Entidad de Certificación Digital.

3.2.3 Autenticación de la identidad individual.

Para asegurar la identidad de una persona natural, la AR **Letmi Ecuador S.A**, exige el registro de la información que demuestre la identidad del solicitante y/o presentación del documento de identidad del solicitante y verifica su existencia y correspondencia contra bases de datos propias y/o de terceros, sean oficiales y/o privadas a través de contratos, convenios, acuerdos, alianzas, y/o cualquier tipo de relación contractual y/o comercial, ya sean directas y/o indirectas. Cuando el servicio es solicitado por un menor de edad, su identidad será asegurada con el documento de identidad y documento que respalde el vínculo del solicitante y el menor de edad. Para el caso que la solicitud se realice por un tercero que confía, se debe entregar escaneada la constancia de delegación del proceso al apoderado. Los documentos se recibirán escaneados, preservando la legibilidad para el uso de la información.

No obstante, lo anterior, ECI **Letmi Ecuador S.A**, se reserva el derecho de emisión de certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial o idoneidad legal o moral de la Entidad de Certificación de Información.

3.2.4 Información de suscriptor no verificada.

En ninguna circunstancia ECI **Letmi Ecuador S.A** omitirá las labores de verificación que conduzcan a la identificación del solicitante y que se traduce en la solicitud y exigencia de la información y/o los documentos mencionados para organizaciones y personas individuales.

Para el caso específico de la dirección de domicilio se presume la buena fe de la información aportada por el solicitante por consiguiente no se realiza verificación de la misma.

3.2.5 Validación de la autoridad.

Letmi Ecuador S.A utiliza un método de comunicación fiable con el solicitante o su representante.

La autoridad de los Solicitantes para solicitar Certificados en nombre de una organización se verifica durante la validación de la identidad del solicitante.

Letmi Ecuador S.A puede permitir que los solicitantes especifiquen por escrito las personas que pueden solicitar certificados digitales en su nombre. Cuando se haya realizado dicha especificación, **Letmi Ecuador S.A** no aceptará solicitudes de certificados que estén fuera de esta especificación pero, previa solicitud por escrito, proporcionará a la empresa solicitante una lista de sus solicitantes de certificados autorizados.

3.2.6 Criterios de interoperabilidad.

ECI **Letmi Ecuador S.A** únicamente emitirá certificados digitales a ECI Subordinadas, donde la toma de decisión de emitir o activar el servicio de certificación digital sea de la ECI **Letmi Ecuador S.A** a través de la recomendación con base en la revisión de la solicitud de la AR de **Letmi Ecuador S.A**.

3.3 Identificación y Autenticación para renovación de llaves.

3.3.1 Identificación y autenticación para la renovación de claves rutinarias.

Letmi Ecuador S.A no considera el proceso de re-uso de las llaves pública y privada del certificado para la renovación de certificados digitales.

En caso de ser solicitada la renovación de un certificado emitido, debe cumplir el proceso de solicitud de emisión de la misma manera que un nuevo certificado, el cual será generado a partir de un nuevo par de llaves.

ECI **Letmi Ecuador S.A** realiza en todos los eventos el proceso de autenticación del solicitante incluso en los de renovación y con base en ello emite los certificados digitales. Lo anterior, a través de cualquier sistema de identificación siempre que subsista contrato, convenio, acuerdo, alianza, y/o cualquier tipo de relación contractual y/o comercial directa y/o indirectamente, entre otras.

3.3.2 Identificación y autenticación para la rutina de re-uso llaves tras la revocación.

Letmi Ecuador S.A no considera el proceso de re-uso de las llaves pública y privada del certificado para la renovación de certificados digitales, cuando haya sido solicitada su revocación.

En caso de ser solicitada la revocación de un certificado emitido y luego se pretende solicitar de nuevo el certificado con los mismos datos del revocado, debe cumplir el proceso de solicitud de emisión de la misma manera que un nuevo certificado, el cual será generado a partir de un nuevo par de llaves.

El proceso de reposición de un certificado de firma digital en consecuencia de la revocación por las diferentes causales definidas en esta DPC, exigen un proceso de verificación para esa solicitud (Reposición).

3.4 Identificación y autenticación para la solicitud de revocación.

Letmi Ecuador S.A atiende las peticiones de revocación de conformidad con las causales de revocación especificadas en el apartado Circunstancias para la revocación de un certificado de esta DPC y autentica la identidad de quien solicita la revocación del certificado. De acuerdo con lo establecido en el procedimiento de revocaciones

4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DEL CERTIFICADO.

4.1 Solicitud de certificado.

Cualquier persona que requiera la prestación del servicio de certificación digital, lo podrá hacer utilizando los canales, medios o mecanismos dispuestos por ECI **Letmi Ecuador S.A**, en los que se obtendrá la información necesaria para gestionar la solicitud del servicio de certificación digital requerido. Una vez aceptados los términos y condiciones y radicada la solicitud, la información es enviada a la Autoridad de Registro quien se encargará de revisar la solicitud para asegurar la identificación inequívoca de la identidad del suscriptor (Persona Natural o Jurídica), la veracidad y autenticidad de la información que permita dar una recomendación para la toma de decisión dando cumplimiento a los requisitos exigidos en las Políticas de Certificación.

De acuerdo a la Ley de Comercio electrónico, firmas y mensajes de datos, “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”. ECI **Letmi Ecuador S.A** determina que los certificados se emitirán desde una CA Subordinada de **Letmi Ecuador S.A** Ecuador.

4.1.1 Quién puede presentar una solicitud de certificado.

Toda persona natural o jurídica legalmente facultada y debidamente identificada puede tramitar la solicitud de emisión de un certificado digital.

4.1.2 Proceso de inscripción y responsabilidades.

La AR de **Letmi Ecuador S.A** previamente cumplidos los requisitos de autenticación y verificación de los datos del solicitante, aprobará y firmará digitalmente la constancia de emisión de los certificados digitales. Toda la información relacionada quedará registrada en el sistema de la AR **Letmi Ecuador S.A**.

4.2 Procesamiento de solicitudes de certificado.

4.2.1 Realizar funciones de identificación y autenticación.

Las funciones de autenticación y verificación de la identidad del solicitante son realizadas por la AR de **Letmi Ecuador S.A**, encargada de dar la recomendación para la toma de la decisión sobre la certificación digital con base en la revisión de la solicitud, quien comprueba si la información suministrada es auténtica y cumple con los requisitos definidos para cada tipo de certificado de acuerdo con esta DPC.

La información y/o documentación que la AR de **Letmi Ecuador S.A** deberá revisar para dar la recomendación para la toma de decisión para la correcta emisión de cada tipo de certificado se define en las Políticas de Certificado de Certificación Digital.

4.2.2 Aprobación o rechazo de solicitudes de certificado

Si una vez verificada la identidad del solicitante, la información suministrada cumple con los requisitos establecidos por esta DPC, se aprueba la solicitud. Si no es posible la identificación plena de la identidad del solicitante o no existe autenticidad plena de la información suministrada, se niega la solicitud y no se emite el certificado digital. ECI **Letmi Ecuador S.A** no asume ninguna responsabilidad por las consecuencias que puedan derivarse de la no aprobación de la emisión de un certificado digital y así lo acepta y reconoce el solicitante al que le haya sido negada la expedición del respectivo certificado.

Igualmente, ECI **Letmi Ecuador S.A** se reserva el derecho de no emitir certificados a pesar de que la identificación del solicitante o la información suministrada por este haya sido plenamente autenticada, cuando la emisión de un certificado en particular por razones de orden legal o de conveniencia comercial, buen nombre o reputación de **Letmi Ecuador S.A** pueda poner en peligro el sistema de certificación digital.

Si posterior a la radicación de una solicitud y el proceso no aprobó la revisión de la solicitud o el solicitante no realizo la validación de identidad, pasados quince (15) días sin que se subsane la novedad, la AR de la ECI **Letmi Ecuador S.A** tendrá como alternativa realizar el rechazo de la solicitud y se notificará al solicitante para que tramite una nueva solicitud.

Para lo cual ECI **Letmi Ecuador S.A** notificará al solicitante la aprobación o rechazo de la solicitud.

4.2.3 Tiempo para procesar las solicitudes de certificado

El plazo para procesar una solicitud por parte de la AR de **Letmi Ecuador S.A**, es de uno (1) a cinco (5) días hábiles desde el momento en que se recibe la información y/o documentación solicitada y el solicitante haya aprobado la validación inicial de la identidad.

4.3 Emisión del Certificado.

4.3.1 Acciones de la AC durante la emisión de certificados.

El paso final del proceso de expedición de certificados digitales es la emisión del certificado por parte de ECI **Letmi Ecuador S.A** y su entrega de manera segura al suscriptor y/o responsable.

La AR de **Letmi Ecuador S.A** genera la documentación formal de la certificación digital, cuando se ha tomado la decisión de otorgar el certificado digital.

El proceso de emisión de certificados digitales vincula de una manera segura la información de registro y la llave pública generada.

4.3.2 Notificación al suscriptor por parte de la AC de la emisión del certificado

Mediante correo electrónico u otro medio definido y autorizado; para tal fin, se notifica al suscriptor la emisión de su certificado digital y por consiguiente el suscriptor acepta y reconoce que una vez reciba la notificación, se entenderá que ha sido emitido el certificado.

La publicación de un certificado en el repositorio de certificados constituye la prueba y una notificación pública de su emisión.

4.4 Aceptación del Certificado.

4.4.1 Conducta que constituye la aceptación del certificado.

No se requiere confirmación por parte del suscriptor o responsable como aceptación del certificado recibido. Se considera que un certificado es aceptado por el suscriptor o responsable desde el momento que solicita su emisión, por ello, si la información contenida en el certificado expedido no corresponde al estado actual de la misma o no fue suministrada correctamente, es responsabilidad del suscriptor informarlo y/o solicitar su revocación.

4.4.2 Publicación del certificado por la AC.

Letmi Ecuador S.A publica todos los certificados de AC en su repositorio y publica los certificados de entidad final entregándolos al suscriptor mediante correo electrónico o una API.
Los certificados de AC subordinadas se entregan a las entidades pertinentes como parte de la cadena de certificados y se publican en su repositorio.

4.4.3 Notificación de la emisión de certificados por parte de la AC a otras entidades.

Véase el apartado 4.4.2. anterior.

Las AR, **Letmi Ecuador S.A** y otras entidades pueden ser informadas de la emisión si participaron en la inscripción inicial

4.5 Uso de pares de claves y certificados.

4.5.1 Uso de la clave privada y el certificado del suscriptor.

El suscriptor o responsable del certificado digital y de la llave privada asociada, acepta las condiciones de uso establecidas en esta DPC por el solo hecho de haber solicitado la emisión del certificado y solo podrá emplearlos para los usos explícitamente mencionados y autorizados en la presente DPC y de acuerdo con lo establecido en los campos “Key Usage” de los certificados. Por consiguiente, los certificados emitidos y la llave privada no deberán ser usados en otras actividades que estén por fuera de los usos mencionados. Una vez expirada la vigencia del certificado, el suscriptor o responsable está obligado a no seguir usando la llave privada asociada al mismo. Con base en lo anterior, desde ya acepta y reconoce el suscriptor, que en tal sentido será el único responsable por cualquier perjuicio pérdida o daño que cause a terceros por el uso de la llave privada una vez expirada la vigencia del certificado. ECI **Letmi Ecuador S.A** no asume ningún tipo de responsabilidad por los usos no autorizados.

Para RSA se tienen definidos los siguientes tamaños de las llaves:

- ECI Raíz de ***ECI LETMI ECUADOR S.A CA*** es de 4096 bits.
- Subordinadas de ECI **Letmi Ecuador S.A** es de 4096 bits.
- Certificados emitidos por ECI **Letmi Ecuador S.A** a usuarios finales es de 2048 bits.

El algoritmo hash de firma es el SHA256 para todos los certificados.

Para el caso de la generación del par de llaves se lleva a cabo en un dispositivo HSM de propiedad de la ECI **Letmi Ecuador S.A** y se le hace entrega al suscriptor y/o responsable de un conjunto de credenciales (usuario y contraseña) para el uso exclusivo de las mismas.

4.5.2 Uso de certificados y claves públicas del tercero que confía.

El suscriptor al que se le haya expedido un certificado se obliga a que cada vez que haga uso del certificado con destino a terceras personas deberá informarles que es necesario que consulten el estado del certificado en la lista de revocación de certificados, así como en el de emitidos a fin de verificar su vigencia y que se esté aplicando dentro de sus usos permitidos establecidos en esta DPC.

En este sentido deberá:

- Comprobar que el certificado asociado no incumple las fechas de inicio y final de vigencia.
- Comprobar que el certificado asociado a la llave privada no está revocado.
- Comprobar que la huella digital (***fingerprint)*** del certificado de la ECI raíz y la del certificado de la subordinada de ECI **Letmi Ecuador S.A** coinciden con el publicado por **Letmi Ecuador S.A** en su página Web.

Huella digital (fingerprint) del certificado Raíz de la ECI Letmi Ecuador S.A:

SHA 256

Fingerprint=A5:ED:DC:A5:8C:51:56:BB:AA:F3:20:12:7A:E7:66:32:32:66:1A:4F:A2:23:FB:71:21:52:96:94:85:E7:45:35

Huella digital (fingerprint) del certificado de la subordinada de ECI Letmi Ecuador S.A:

SHA 256

Fingerprint=D1:ED:59:23:3B:D3:4E:FE:6B:97:D6:4C:D4:C1:69:94:15:1F:0E:8D:CD:8D:A3:CE:27:F1:24:CC:C3:61:4D:8F

4.6 Renovación del certificado

La ECI Letmi Ecuador S.A., no atiende requerimientos de renovación de un certificado sin cambio de llaves.

4.6.1 Circunstancias para la renovación de certificado.

No aplica por cuanto no se expiden certificados sin cambio de llaves.

4.6.2 Quién puede solicitar una renovación sin cambio de llaves.

No aplica por cuanto no se expiden certificados sin cambio de llaves.

4.6.3 Trámites para la solicitud de renovación de certificados.

No aplica por cuanto no se expiden certificados sin cambio de llaves.

4.6.4 Notificación al suscriptor o responsable de la emisión de un nuevo certificado sin cambio de llaves.

No aplica por cuanto no se expiden certificados sin cambio de llaves.

4.6.5 Forma en la que se acepta la renovación de un certificado.

No aplica por cuanto no se expiden certificados sin cambio de llaves.

4.6.6 Publicación del certificado renovado por la ECI.

No aplica por cuanto no se expiden certificados sin cambio de llaves.

4.6.7 Notificación de la emisión de un certificado renovado por la ECI a otras entidades.

No aplica por cuanto no se expiden certificados sin cambio de llaves.

4.7 Re-uso de clave del certificado

Letmi Ecuador S.A trata todas las solicitudes de re-emisión y/o renovación de certificados como solicitudes de emisión de un nuevo certificado, teniendo en cuenta que no hace en ningún caso re-uso de llaves.

4.7.1 Circunstancia para el re-uso de claves del certificado.

No aplica por cuanto no se expiden certificados sin cambio de llaves.

4.7.2 Quién puede solicitar la certificación de una nueva clave pública.

No aplica por cuanto no se expiden certificados sin cambio de llaves.

4.7.3 Procesamiento de las solicitudes de re-uso de clave de certificados.

No aplica por cuanto no se expiden certificados sin cambio de llaves.

4.7.4 Notificación al suscriptor de la emisión de un nuevo certificado.

No aplica por cuanto no se expiden certificados sin cambio de llaves.

4.7.5 Conducta que constituye la aceptación de un certificado con re-uso de clave.

No aplica por cuanto no se expiden certificados sin cambio de llaves.

4.7.6 Publicación del certificado con re-uso de clave por parte de la AC

No aplica por cuanto no se expiden certificados sin cambio de llaves.

4.7.7 Notificación de la emisión de certificados por parte de la AC a otras entidades

No aplica por cuanto no se expiden certificados sin cambio de llaves.

4.8 Modificación del Certificado.

Los certificados digitales emitidos por ECI **Letmi Ecuador S.A** no puede ser modificados, es decir, no aplican enmiendas. En consecuencia, el suscriptor debe solicitar la emisión de un nuevo certificado digital. En este evento se expedirá un nuevo certificado al suscriptor; el costo de esta modificación será asumido completamente por el suscriptor conforme a las tarifas informadas por ECI **Letmi Ecuador S.A** o según las condiciones definidas a nivel contractual.

4.8.1 Circunstancias para la modificación del certificado.

No aplica ya que los certificados digitales emitidos por ECI **Letmi Ecuador S.A** no pueden ser modificados.

4.8.2 Quién puede solicitar la modificación del certificado.

No aplica ya que los certificados digitales emitidos por ECI **Letmi Ecuador S.A** no pueden ser modificados.

4.8.3 Tramitación de solicitudes de modificación de certificados.

No aplica ya que los certificados digitales emitidos por ECI **Letmi Ecuador S.A** no pueden ser modificados.

4.8.4 Notificación al suscriptor de la emisión de un nuevo certificado

No aplica ya que los certificados digitales emitidos por ECI **Letmi Ecuador S.A** no pueden ser modificados.

4.8.5 Conducta que constituye la aceptación de un certificado modificado.

No aplica ya que los certificados digitales emitidos por ECI **Letmi Ecuador S.A** no pueden ser modificados.

4.8.6 Publicación del certificado modificado por la AC.

No aplica ya que los certificados digitales emitidos por ECI **Letmi Ecuador S.A** no pueden ser modificados.

4.8.7 Notificación de la emisión de certificados por parte de la AC a otras entidades.

No aplica ya que los certificados digitales emitidos por ECI **Letmi Ecuador S.A** no pueden ser modificados.

4.9 Revocación y suspensión del certificado.

4.9.1 Circunstancias para revocación.

El suscriptor o responsable puede voluntariamente solicitar la revocación de su certificado digital en cualquier instante conforme a lo descrito en la Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos, vigente, pero está obligado a solicitar la revocación de su certificado digital bajo las siguientes situaciones:

1. Por pérdida o inutilización de la clave privada o certificado digital.
2. La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido.
3. Cambios en las circunstancias por la cuales ECI **Letmi Ecuador S.A** autorizó la emisión del certificado digital.
4. Si durante el periodo de vigencia parte o toda la información contenida en el certificado digital pierde actualidad o validez.

Si el suscriptor o responsable no solicita la revocación del certificado en el evento de presentarse las anteriores situaciones, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe exenta de culpa que confiaron en el contenido del certificado.

El suscriptor o responsable reconoce y acepta que los certificados deben ser revocados cuando **Letmi Ecuador S.A** conoce o tiene indicios o confirmación de ocurrencia de alguna de las siguientes circunstancias:

1. A petición del suscriptor, responsable o un tercero en su nombre y representación.
2. Por muerte del suscriptor o responsable.
3. Por la confirmación o evidencia de que alguna información o hecho contenido en el certificado digital es falso.
4. La clave privada de la entidad de certificación o su sistema de seguridad ha sido comprometida de manera material que afecte la confiabilidad del certificado.
5. Por orden judicial o de entidad administrativa competente.
6. Por compromiso de la seguridad en cualquier motivo, modo, situación o circunstancia.
7. Por incapacidad sobrevenida del suscriptor o responsable.

8. Por liquidación de la persona jurídica representada que consta en el certificado digital.
9. Por la ocurrencia de hechos nuevos que provoquen que los datos originales no correspondan a la realidad.
10. Por la terminación del contrato de suscripción, de conformidad con las causales establecidas en el contrato.
11. Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto de que se ponga en duda la confiabilidad del certificado digital.
12. Por el manejo indebido por parte del suscriptor del certificado digital.
13. Por el incumplimiento del suscriptor o de la persona jurídica que representa o a la que está vinculado a través del documento términos y condiciones o responsable de certificados digitales de la ECI **Letmi Ecuador S.A**.
14. Conocimiento de eventos que modifiquen el estado inicial de los datos suministrados, entre otros: terminación de la Representación Legal, terminación del vínculo laboral, liquidación o extinción de la personería jurídica, cesación en la función pública o cambio a una distinta.
15. En cualquier momento que se evidencie falsedad en los datos suministrados por el solicitante, suscriptor o responsable.
16. Por incumplimiento por parte de la ECI **Letmi Ecuador S.A**, el suscriptor o responsable de las obligaciones establecidas en la DPC.
17. Por incumplimiento en el pago de los valores por los servicios de certificación, acordados entre el solicitante y ECI **Letmi Ecuador S.A**. No obstante, las causales anteriores, ECI **Letmi Ecuador S.A**, también podrá revocar certificados cuando a su juicio se pueda poner en riesgo la credibilidad, confiabilidad, valor comercial, buen nombre de la ECI **Letmi Ecuador S.A**, idoneidad legal o moral de todo el sistema de certificación.

4.9.2 Quién puede solicitar la revocación de un certificado.

El suscriptor o responsable, un tercero de buena fe o cualquier persona interesada cuando tenga constancia demostrable de conocimiento de hechos y causales de revocación mencionadas en el apartado Circunstancias para la revocación de un certificado de esta DPC y que comprometan la llave privada.

Un tercero de buena fe o cualquier persona interesada que tenga constancia demostrable que un certificado digital ha sido empleado con fines diferentes a los expuestos en el aparte Usos adecuados del certificado de esta DPC.

Cualquier persona interesada que tenga constancia demostrable que el certificado no está en poder del suscriptor o responsable.

El equipo de Tecnología de la CA como máximo ente de control que tiene atribuida la administración de la seguridad de la infraestructura tecnológica de la ECI **Letmi Ecuador S.A**, está en capacidad de solicitar la revocación de un certificado si tuviera el conocimiento o sospecha del compromiso de la llave privada del suscriptor, responsable o cualquier otro hecho de acuerdo con las circunstancias para la revocación de un certificado.

4.9.3 Procedimiento para solicitud de revocación de un certificado.

El suscriptor y/o responsable, un tercero de buena fe o cualquier persona tendrán la oportunidad de solicitar la revocación de un certificado digital cuyas causas están especificadas en esta DPC lo pueden hacer bajo los siguientes procedimientos:

- En las oficinas de **Letmi Ecuador S.A**.

En horario de atención al público se reciben las solicitudes escritas de revocación de certificados digitales firmadas por los suscriptores y/o responsables suministrando el documento de identificación original.

- Solicitud de revocación en línea:

El suscriptor y/o responsable, podrá llevar a cabo el proceso de revocación del certificado digital por medio del portal web de **Letmi Ecuador S.A**, https://letmi.app/ - Solicite su revocación, al diligenciar la solicitud se visualizarán los certificados digitales vigentes, se debe seleccionar el certificado a revocar y a su correo electrónico registrado, le llegará una notificación con el código de seguridad para completar el diligenciamiento de la solicitud de revocación en línea, el suscriptor y/o responsable deberá seleccionar el motivo de la revocación, ingresar el código de seguridad y envía la solicitud de revocación de su certificado digital; una vez la solicitud termine, se realizará la revocación de su certificado digital y al correo electrónico registrado se le enviará la notificación de revocación.

Otros medios dispuestos para realizar la revocación del certificado digital por parte del suscriptor y/o responsable y/o tercero de buena fe podrán ser a través de la(s) herramienta(s) y/o aplicación(es) desde donde se radicó la solicitud para la emisión del certificado digital de terceros autorizados.

Servicio de Revocación vía correo electrónico:

Por medio de nuestro correo electrónico info@letmi.app, los suscriptores y/o responsables pueden solicitar la revocación de certificados digitales conforme a las causales de revocación mencionadas en el apartado Circunstancias para la revocación de un certificado de esta DPC, enviando carta de solicitud de revocación digital firmada o correo electrónico con los datos del suscriptor y causal de revocación.

4.9.4 Periodo de gracia para solicitar revocación de un certificado.

Previa revisión de una solicitud de revocación la ECI **Letmi Ecuador S.A** procederá en forma inmediata con la revocación solicitada, dentro de los horarios de oficina de éste. En consecuencia, no existe un periodo de gracia que permita al solicitante cancelar la solicitud. Si se trató de una solicitud errónea, el suscriptor o responsable debe solicitar un nuevo certificado, pues el certificado revocado perdió su validez inmediatamente fue validada la solicitud de revocación y la ECI **Letmi Ecuador S.A** no podrá reactivarlo.

El procedimiento utilizado por la ECI **Letmi Ecuador S.A** para verificar una solicitud de revocación formulada por una persona determinada, es revisar la solicitud de acuerdo con el apartado anterior.

Una vez solicitada la revocación del certificado, si se evidencia que dicho certificado es utilizado vinculado con la llave privada, el suscriptor o responsable releva de toda responsabilidad legal a la ECI **Letmi Ecuador S.A**, toda vez que reconoce y acepta que el control, custodia y confidencialidad de la llave privada es responsabilidad exclusiva de este.

4.9.5 Tiempo dentro del cual la AC debe procesar la solicitud de revocación.

La solicitud de revocación de un certificado digital debe ser atendida con la máxima prioridad, sin que su revocación tome más de tres (3) días hábiles una vez revisada la solicitud.

Una vez cumplidas las formalidades previstas para la revocación y si por alguna razón, no se hace efectiva la revocación de un certificado en los términos establecidos por esta DPC, la ECI **Letmi Ecuador S.A** como prestador de servicios de certificación y responsable de la CA, responderá por los perjuicios que se causen a los suscriptores o terceros de buena fe derivados de errores y omisiones, de mala fe de los administradores, representantes legales o empleados de la ECI **Letmi Ecuador S.A** en el desarrollo de las actividades para las cuales cuenta con autorización y para ello cuenta con un seguro de responsabilidad civil de conformidad con el Art. 30 de la Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos. La ECI **Letmi Ecuador S.A** no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante el suscriptor y/o responsables del certificado o terceros de confianza a excepción de lo establecido por las disposiciones de la presente DPC.

4.9.6 Requisito de comprobación de revocación para las partes confiantes.

Es responsabilidad del suscriptor y/o responsable de un certificado digital y éste así lo acepta y reconoce, informar a los terceros de buena fe de la necesidad de comprobar la validez de los certificados digitales sobre los que esté haciendo uso en un momento dado. Informará igualmente el suscriptor y/o responsable al tercero de buena fe que, para realizar dicha consulta, dispone de la lista de certificados revocados CRL, publicada de manera periódica por la ECI **Letmi Ecuador S.A**.

Las partes confiantes deben confirmar la validez de cada certificado de la cadena de certificación, comprobando la CRL o el respondedor OCSP correspondiente antes de confiar en un certificado emitido por la CA de la ECI **Letmi Ecuador S.A**.

4.9.7 Frecuencia de emisión de las CRLs.

La ECI **Letmi Ecuador S.A** generará y publicará para sus entidades subordinadas una nueva CRL cada veinticuatro (24) horas en su repositorio con una disponibilidad de consulta en línea 7×24×365, 99.8% uptime por año; para las entidades Raíz el periodo de generación se establece en (1) año.

4.9.8 Latencia máxima de las CRLs.

El tiempo entre la generación y publicación de la CRL es mínimo debido a que la publicación es automática.

4.9.9 Disponibilidad de verificación en línea de revocación/estado.

La ECI **Letmi Ecuador S.A** publicará tanto la CRL como el estado de los certificados revocados en repositorios de libre acceso y fácil consulta, con disponibilidad 7X24 durante todos los días del año. ECI **Letmi Ecuador S.A** ofrece un servicio de consulta en línea basada en el protocolo OCSP en la dirección http://ocsp.letmi.app

La validación en línea de certificados digitales mediante OCSP se debe realizar con una herramienta que implemente el protocolo OCSP y sea capaz de entender las respuestas generadas por el servicio, tal es el caso de OPENSSL.

4.9.10 Requisitos de comprobación de revocación en línea.

Para obtener la información del estado de revocación de un certificado en un momento dado, se puede hacer la consulta en línea en la dirección http://ocsp.letmi.app para lo cual se debe contar con un software que sea capaz de operar con el protocolo RFC6960. La mayoría de los navegadores ofrecen este servicio.

La validación en línea de certificados digitales mediante OCSP se debe realizar con una herramienta que implemente el protocolo OCSP y sea capaz de entender las respuestas generadas por el servicio, tal es el caso de OPENSSL.

4.9.11 Otras formas de anuncios de revocación disponibles.

Dentro de las 24 horas siguientes a la revocación de un certificado, la ECI **Letmi Ecuador S.A** informa al suscriptor y/o responsable mediante correo electrónico u otro medio para tal fin se notifica la revocación de su certificado digital y por consiguiente el solicitante acepta y reconoce que una vez reciba la notificación se entenderá que su solicitud fue atendida. Se entenderá que se ha recibido la información donde se notifica la revocación de un certificado cuando dicha notificación ingrese en el sistema de información designado por el solicitante.

La publicación de un certificado revocado en la CRL constituye la prueba y una notificación pública de su revocación.

La ECI **Letmi Ecuador S.A** mantendrá un archivo histórico hasta de tres (3) años de las CRL´s generadas y que estarán a disposición de los suscriptores mediante solicitud escrita dirigida a la ECI **Letmi Ecuador S.A.**

4.9.12 Requisitos especiales en materia de compromiso de claves.

Si se solicitó la revocación de un certificado digital por compromiso (pérdida, destrucción, robo, divulgación) de la llave privada, el suscriptor puede solicitar un nuevo certificado digital por un periodo igual o mayor al inicialmente solicitado presentando una solicitud de renovación en relación con el certificado digital comprometido. La responsabilidad de la custodia de la llave es del suscriptor o responsable y éste así lo acepta y reconoce, por tanto, es él quien asume el costo de la renovación de conformidad con las tarifas vigentes fijadas para la renovación de certificados digitales.

En caso de que la llave privada del suscriptor se vea comprometida, el suscriptor deberá notificar inmediatamente a la ECI **Letmi Ecuador S.A** el evento de compromiso de la llave privada. La ECI **Letmi Ecuador S.A** revocará el certificado en cuestión y publicará una CRL para informar a las partes usuarias de que el certificado ya no es de confianza.
El suscriptor es responsable de investigar las circunstancias de dicho compromiso.

4.9.13 Circunstancias para la suspensión

ECI **Letmi Ecuador S.A** no dispone del servicio de suspensión de certificados digitales, únicamente revocación.

4.9.14 Quién puede solicitar la suspensión

No aplica por cuanto ECI **Letmi Ecuador S.A** no dispone del servicio de suspensión de certificados digitales, únicamente revocación.

4.9.15 Procedimiento de solicitud de suspensión

No aplica por cuanto ECI **Letmi Ecuador S.A** no dispone del servicio de suspensión de certificados digitales, únicamente revocación.

4.9.16 Límites del periodo de suspensión

No aplica por cuanto ECI **Letmi Ecuador S.A** no dispone del servicio de suspensión de certificados digitales, únicamente revocación.

4.10 Servicios de Estado de los Certificados.

4.10.1 Características operativas

Para la consulta del estado de los certificados emitidos por ECI **Letmi Ecuador S.A**, se dispone de un servicio de consulta en línea basada en el protocolo OCSP en la dirección http://ocsp.letmi.app. El suscriptor o responsable de enviar una petición de consulta sobre el estado del certificado a través del protocolo OCSP, que, una vez consultada la base de datos, es atendida mediante una respuesta vía http o la consulta vía CRL.

Las CRLs emitidas por la ECI **Letmi Ecuador S.A** cumplen con la RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and CRL Profile V2” y contienen los siguientes elementos básicos:

Número de versión.

Las CRL´s emitidas por ECI **Letmi Ecuador S.A** cumplen con el estándar X.509 vigente.

CRL y extensiones CRL.

La información sobre el motivo de la revocación de un certificado estará incluida en la CRL, utilizando las extensiones de la CRL y más específicamente en el campo de motivos de revocación (reasonCode).

Disponibilidad CRL.

Conforme a lo indicado en el numeral 4.9.9 Disponibilidad de verificación en línea de revocación/estado.

Perfil OCSP.

El servicio OCSP cumple con lo estipulado en el RFC6960 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”.

Número de versión.

Cumple con la OCSP Versión 1 del RFC6960 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”.

Extensiones OCSP.

No aplica.

Disponibilidad servicio OCSP.

Conforme a lo indicado en el numeral 4.9.9 Disponibilidad de verificación en línea de revocación/estado.

4.10.2 Disponibilidad servicio

La **Letmi Ecuador S.A** ECI opera y mantiene su capacidad CRL y OCSP con recursos suficientes para proporcionar un tiempo de respuesta de diez segundos o menos en condiciones normales de funcionamiento.
Los servicios de estado de certificados están disponibles 24 horas al día, 7 días a la semana, a menos que no estén disponibles temporalmente debido a tareas de mantenimiento o a un fallo del servicio. Además, La ECI **Letmi Ecuador S.A** mantiene una capacidad de respuesta interna ininterrumpida a los informes de problemas de certificados de alta prioridad.

4.10.3 Características opcionales.

Para obtener la información del estado de certificado en un momento dado, se puede hacer la consulta en línea en la dirección http://ocsp.letmi.app, para lo cual se debe contar con un software que sea capaz de operar con el protocolo OCSP. La mayoría de los navegadores ofrecen este servicio o consulta a la CRL publicada en el portal https://crl.letmi.app/

La validación en línea de certificados digitales mediante OCSP se debe realizar con una herramienta que implemente el protocolo OCSP y sea capaz de entender las respuestas generadas por el servicio, tal es el caso de OPENSSL.

4.11 Fin de la Suscripción.

ECI **Letmi Ecuador S.A** da por finalizada la vigencia de un certificado digital emitido ante las siguientes circunstancias:

- Pérdida de validez por revocación del certificado digital.
- Vencimiento del periodo para el cual un suscriptor contrató la vigencia del certificado.

4.12 Custodia y Recuperación de claves

4.12.1 Política y prácticas en materia de custodia y recuperación de llaves.

La clave privada del suscriptor solo puede ser almacenada en un dispositivo criptográfico hardware (HSM).

Los dispositivos criptográficos en hardware utilizados por la ECI **Letmi Ecuador S.A** cumplen con las certificaciones como chip criptográfico: nivel de seguridad CC EAL5+ PP 9806, BSI-PP-002-2001, FIPS 140-2 NIVEL 3 y las certificaciones SO del chip criptográfico: nivel de seguridad CC EAL4+ BSI-PP-0006-2002 (CWA 14169 SSCD Type-3) – BSI –DSZ-CC-0422-2008 y soportan los estándares PKCS#11, Microsoft CAPI, PC/SC, X.509 vigente certificate storage, SSL v3, IPsec/IKE.

La ECI **Letmi Ecuador S.A** publica en las Políticas de Certificado Digital para Certificados Digitales las características de los dispositivos criptográficos que ofrece a los suscriptores que así lo solicitan para creación y almacenamiento de sus claves privadas.

Políticas de custodia y recuperación de llaves.

La generación de la llave privada es almacenada sobre un dispositivo seguro (hardware), del cual no se puede exportar. En consecuencia, no es posible la recuperación de la llave privada del suscriptor. La responsabilidad de la custodia de la llave privada es del suscriptor y éste así lo acepta y reconoce.

4.12.2 Política y prácticas de encapsulación y recuperación de claves de sesión.

La recuperación de la clave de sesión del suscriptor o PIN no es posible ya que el único responsable de asignarla y este así lo declara y acepta. La responsabilidad de la custodia de la clave de sesión o PIN es del suscriptor quien acepta no mantener registros digitales, escritos o en cualquier otro formato y quien se obliga a proteger el acceso al PIN, por lo que si se presenta olvido del PIN se radicará un caso en la mesa de servicios de la ECI – **Letmi Ecuador S.A** para verificar la solicitud y de ser requerido se el suscriptor radicará una solicitud de revocación del certificado y gestionará la solicitud de un nuevo certificado digital.

5. INSTALACIONES, GESTIÓN Y CONTROLES OPERATIVOS.

5.1 Controles Físicos.

La infraestructura de AC de la ECI **Letmi Ecuador S.A** se encuentra en instalaciones seguras y se gestiona desde ellas. Existen y se siguen procedimientos de seguridad detallados que prohíben el acceso y la entrada no autorizados a las áreas de las instalaciones en las que residen los sistemas de AC.

5.1.1 Ubicación y construcción del sitio.

La ECI **Letmi Ecuador S.A** dispone de medidas de seguridad para el control de acceso al edificio donde se encuentra su infraestructura, los servicios de certificación digitales regulados y prestados a través de esta DPC se realizan a través de un proveedor de servicios. Solo se permite el acceso al rack que alberga los servidores a través del cual se manejan los servicios de comunicación de la ECI **Letmi Ecuador S.A** de personas previamente identificadas y autorizadas que porten en un lugar visible el carné de visitantes.

La ECI **Letmi Ecuador S.A** garantiza que los servidores de la PKI se encuentran en operación continúa de manera virtual en la nube de Amazon.

Dicho proveedor cuenta con procedimientos para realizar las operaciones de administración de la infraestructura de comunicaciones de la ECI **Letmi Ecuador S.A** y a donde únicamente tiene acceso el personal autorizado.

El área restringida del centro de comunicaciones cumple con los siguientes requisitos:

1. Ingresan únicamente personas autorizadas.
2. Los equipos de comunicación crítica están debidamente protegidos en racks.
3. No posee ventanas hacia el exterior del edificio.
4. Se monitorea a través de un circuito cerrado de televisión las 24 horas, con cámaras tanto al interior como al exterior del centro de cómputo.
5. Cuenta con control de acceso físico.
6. Sistemas de protección y prevención de incendios: detectores de humo, sistema de extinción de incendios.
7. Cuenta con personal capacitado para actuar ante eventos catastróficos.
8. Cuenta con un sistema detector de intrusos físicos.
9. El cableado está debidamente protegido contra daños, intentos de sabotaje o interceptación por medio de canaletas

5.1.2 Acceso físico.

Existen varios niveles de seguridad que restringen el acceso a la infraestructura de comunicaciones a través de la cual ECI **Letmi Ecuador S.A** presta sus servicios y cada uno ellos disponen de sistemas de control de acceso físico. Las instalaciones cuentan con un servicio de circuito cerrado de televisión y con personal de vigilancia. Existen dentro de las instalaciones zonas restringidas que por el tipo de equipos de comunicaciones considerados críticos y operaciones sensibles que se manejan tienen acceso permitido solo a ciertas personas.

5.1.3 Energía y aire acondicionado.

El centro de comunicaciones cuenta con un sistema de aire acondicionado y dispone de un adecuado suministro de electricidad con protección contra caídas de tensión y otras fluctuaciones eléctricas que podrían eventualmente afectar sensiblemente a los equipos y producir daños graves. Adicionalmente, se cuenta con un sistema de respaldo que garantiza que no haya interrupción en el servicio con una autonomía suficiente para garantizar la continuidad en el servicio. En caso de una falla en el sistema de respaldo, se cuenta con el tiempo suficiente para hacer un apagado controlado.

5.1.4 Exposición al agua.

Los centros de datos donde se encuentran alojados los servicios de PKI cuentan con aislamientos de posibles fuentes de agua y cuentan con sensores de detección de inundaciones conectados al sistema general de alarma.

5.1.5 Prevención y protección contra incendios.

El centro de comunicaciones cuenta de un sistema de detección y extinción de incendios. Se cuenta con un sistema de cableado que protege las redes internas.

5.1.6 Almacenamiento de medios.

Se cuenta con procedimientos de toma de backups, restauración y pruebas para las bases de datos para los servicios acreditados.

Los servidores misionales se encuentran en ambientes cloud, sin embargo, a los servidores onpremises se les realizan los backups.

5.1.7 Eliminación de residuos

Todo documento en papel que contenga información sensible de la entidad y que ha cumplido su vida útil deberá ser destruido físicamente para garantizar la imposibilidad de recuperación de información. Si el documento o información está almacenado en un medio magnético se debe formatear, borrar permanentemente o destruir físicamente el dispositivo en casos extremos como daños de dispositivos de almacenamiento o dispositivos no reutilizables, siempre garantizando que no sea posible la recuperación de la información por cualquier medio conocido o no conocido por el momento.

5.1.8 Copia de seguridad fuera de sitio.

ECI **Letmi Ecuador S.A** mantendrá una copia de respaldo de las bases de datos en Amazon que se llevará a la réplica en caso de que se requiera para la restauración.

Controles físicos de la infraestructura tecnológica a través de la cual ECI Letmi Ecuador S.A presta sus servicios

Los servicios de infraestructura tecnológica a través de la cual ECI **Letmi Ecuador S.A** presta sus servicios.

5.2 Controles de Procedimiento.

5.2.1 Roles de confianza.

La AR ha definido los siguientes roles, los cuales no podrán ser desempañados por la misma persona dentro del área:

- **Agentes de la AR:** Personas responsables de las operaciones diarias tales como los son: revisión y aprobación de las solicitudes atendiendo todas las actividades relacionadas con los servicios de certificación digital prestados por la ECI **Letmi Ecuador S.A** a través de la RA, las funciones y responsabilidades de los agentes de la AR están definidos de acuerdo con los Perfiles y Funciones de la ECI **Letmi Ecuador S.A**.
- **Administrador AR:** La persona responsable por administrar y configurar la AR.
- **Auditor AR :** Persona capacitada e imparcial encargada de evaluar el cumplimiento de los requisitos de la AR, auditando los sistemas de información de la AR aclarando que su rol es distinto al del auditor interno de los sistemas de gestión.
- **Ingeniero de sistemas de infraestructura**: autorizado para instalar, configurar y mantener los sistemas de AC utilizados para la gestión del ciclo de vida de los certificados.
- **Operador de Infraestructura:** Responsable de operar los sistemas de AC en el día a día. Autorizado para realizar copias de seguridad/recuperación del sistema, visualización/mantenimiento de archivos del sistema AC y registros de auditoría.
- **Especialistas en Validación:** Responsables de validar la autenticidad e integridad de los datos a ser incluidos dentro de los Certificados a través de un sistema AR adecuado y aprobar la generación/suspensión de Certificados.
- **Oficial de seguridad/Jefe de seguridad de la información**: Responsabilidad general de administrar la implementación de las prácticas de seguridad de la AC.

5.2.2 Número de personas necesarias por tarea.

Para cada uno de los roles mencionados la ECI garantizará los colaboradores para realizar las tareas que afectan a la gestión de claves criptográficas de la propia ECI.

5.2.3 Identificación y autenticación de cada rol.

Los Agentes AR y Administrador AR se autentican mediante certificados digitales emitidos por ECI **Letmi Ecuador S.A**.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante login/ password, certificados digitales.

5.2.4 Roles que requieren segregación de funciones.

El rol de Administrador AR, los Agentes de la AR y Auditor AR son independientes.

5.3 Controles de personal.

5.3.1 Cualificaciones, experiencia y requisitos de habilitación

Se tiene definido un proceso de selección de personal que tiene como base el perfil de cada uno de los cargos involucrados en el proceso de emisión de certificados digitales y los procedimientos de servicios de certificación digital. El candidato a un cargo debe tener la educación, formación, experiencia y habilidades definidas en el documento Perfil y Funciones de cargo.

5.3.2 Procedimiento de verificación de antecedentes.

Los candidatos a ocupar cargos del ciclo de certificación deben presentar su certificado de antecedentes vigente, según se tiene establecido en los procesos internos de talento humano de la ECI **Letmi Ecuador S.A**.

5.3.3 Requisitos de formación.

Letmi Ecuador S.A realizan los cursos necesarios a sus empleados y a los operadores de registro, para asegurarse de la correcta realización de las tareas de certificación, especialmente cuando se realicen modificaciones sustanciales en las mismas y en función de los conocimientos personales de cada operador.

5.3.4 Requisitos y frecuencia de actualización de formación.

Dentro de la programación anual de capacitación se incluye una actualización en Seguridad de la Información para los integrantes del Ciclo de emisión de certificados digitales.

5.3.5 Frecuencia y secuencia de rotación de tareas.

No existe rotación de tareas en los cargos mencionados.

5.3.6 Sanciones por acciones no autorizadas.

Es calificada como falta grave ejecutar acciones no autorizadas y las personas serán sancionadas de conformidad con reconvención y/o proceso disciplinario.

5.3.7 Requisitos para contratación de terceros.

Entre los requisitos de contratación de terceros está el conocimiento de las Políticas de Seguridad y una cláusula de confidencialidad sobre la información que sea suministrada o conocida por razones del vínculo contractual con **Letmi Ecuador S.A**.

5.3.8 Documentación suministrada al personal.

El prestador de servicios de certificación suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de realizar su trabajo de forma competente y satisfactoria.

5.4 Procedimientos de Registro de Auditoría.

Los procedimientos de auditoría de seguridad son ejecutados internamente o por proveedores de auditoría de tercera parte.

5.4.1 Tipo de eventos registrados.

Se generarán archivos de registro de auditoría para todos los eventos relacionados con la seguridad y los servicios de la AC. Siempre que sea posible, los registros de auditoría de seguridad se generarán automáticamente.

Las actividades más sensibles del ciclo de certificación requieren el control y seguimiento de eventos que se pueden presentar durante su operación. De conformidad con su nivel de criticidad los eventos se clasifican en:

- Informativo: Una acción terminó de manera exitosa
- Tipo marca: Inicio y finalización de una sesión
- Advertencia: Presencia de un hecho anormal pero no de una falla
- Error: Una operación generó una falla predecible
- Error fatal: Una operación generó una falla impredecible

5.4.2 Frecuencia de procesamiento de Logs.

Los registros de auditoria son revisados utilizando procedimientos manuales y/o automáticos.

La revisión de los logs se realiza una vez por semana o cuando se detecte una alerta de seguridad o existan indicios de un funcionamiento no usual de los sistemas.

5.4.3 Periodo de retención de los registros de auditoría.

Los registros de auditoría se mantienen durante tres (3) años después de la última modificación del fichero, con eso se garantiza poder revisar los problemas presentados con los que se hayan presentado en el histórico. Una vez transcurridos los 3 años y con autorización de las partes interesadas de **Letmi Ecuador S.A**, puede proceder a destruirlos, no obstante, si los registros se están utilizando en procesos judiciales su retención serán por tiempo indefinido.

5.4.4 Protección de los registros de auditoría.

Los logs de auditoría del sistema de información se conservan de igual manera manteniendo una copia en el sitio y otra copia fuera de las instalaciones.

5.4.5 Procedimiento de copia de seguridad de los registros de auditoría.

Los backups de los registros de auditoria se replican a un sitio de logs centralizados

5.4.6 Sistema de recopilación de auditorías (interna o externa)

El sistema de recopilación de información de auditoría se basa en los registros automáticos de las aplicaciones que soportan el ciclo de certificación incluyendo los logs de aplicación, logs de seguridad y logs del sistema. Los cuales se almacenan en CloudWatch y bases de datos para su monitoreo

5.4.7 Notificación al sujeto causante del incidente de seguridad

A juicio del Oficial de Seguridad de la Información, se hará la notificación al sujeto causa de un incidente de seguridad detectado a través de los logs de auditoría a fin de tener respuesta formal sobre lo sucedido.

5.4.8 Evaluaciones de vulnerabilidad.

Además de las revisiones periódicas de logs, ECI **Letmi Ecuador S.A** realiza de manera esporádica o ante actividades sospechosas la revisión de estos de conformidad con los procedimientos internos establecidos. De igual manera revisa los resultados obtenidos del Ethical Hacking y las actividades descritas para subsanación de hallazgos

5.5 Archivo de Registros.

El registro de archivo y registro de eventos es ejecutado por el NOC SOC de **Letmi Ecuador S.A**.

5.5.1 Tipos de registros archivados.

Se mantiene un archivo de registros de los eventos más relevantes sobre las operaciones realizadas durante el proceso de emisión de los certificados digitales.

La AC y ARs archivan registros con suficiente detalle para establecer la validez de una firma y el correcto funcionamiento y seguridad del sistema AC.

5.5.2 Periodo de retención para archivo

El período de retención es de 3 años o el periodo que establezca la legislación vigente.

5.5.3 Protección de archivo

Los archivos generados se conservan bajo custodia con estrictas medidas de seguridad para conservar su estado e integridad.

5.5.4 Procedimientos de copia de seguridad de archivos

Las copias de respaldo de los Archivos de registros se realizan según los procedimientos establecidos para copias de respaldo y recuperación de backups del resto de sistemas de información.

5.5.5 Requisitos para el sellado de tiempo de los registros.

Los servidores se mantienen actualizados con la hora UTC Time (tiempo universal coordinado). Están sincronizados mediante el protocolo NTP (Network Time Protocol). La sincronización se realizará con el servidor de NTP del INM.

5.5.6 Sistema de recolección de archivos (interna o externa).

La información de auditoría tanto externa como interna es almacenada y custodiada en un sitio externo a las instalaciones de ECI **Letmi Ecuador S.A.** una vez haya sido digitalizada. Los archivos de auditoría digitalizados son accedidos únicamente por el personal autorizado mediante herramientas de visualización. En Amazon se mantiene en el servicio de CloudWatch bases de datos.

5.5.7 Procedimientos para obtener y verificar información de archivo.

Los archivos de registros son accedidos únicamente por el personal autorizado mediante herramientas de visualización y gestión de eventos con el propósito de verificar integridad de estos o para auditorias ante incidentes de seguridad.

5.6 Cambio de Llaves.

Cambio de llave de la raíz ECI Letmi Ecuador S.A.

El procedimiento de cambio de llaves de la Raíz de ECI **Letmi Ecuador S.A** es el equivalente a generar un nuevo certificado digital. Los certificados emitidos por las subordinadas con la llave anterior deben ser revocados o se debe mantener la infraestructura hasta el vencimiento del último certificado emitido. Si se opta por revocar los certificados y emitir unos nuevos, estos no tendrán costo alguno para el suscriptor o responsable.

Antes de que el uso de la llave privada de ECI **Letmi Ecuador S.A** caduque se realizará un cambio de llaves. La anterior AC raíz y su llave privada solo se usarán para la firma de la CRL mientras existan certificados activos emitidos por las subordinadas de la AC anterior. Se generará una AC raíz con una llave privada nueva y un nuevo DN. La llave pública se publicará en el mismo repositorio con un nombre nuevo que la diferencia de la anterior.

Cambio de llaves de la Subordinada de ECI Letmi Ecuador S.A.

El procedimiento de cambio de llaves de una subordinada de la ECI **Letmi Ecuador S.A** es el equivalente a generar un nuevo certificado digital. Los certificados emitidos con la llave anterior de la subordinada deben ser revocados o se debe mantener la infraestructura hasta el vencimiento del último certificado emitido. Si se opta por revocar los certificados y emitir unos nuevos, estos no tendrán costo alguno para el suscriptor o responsable.

Antes de que el uso de la llave privada de la subordinada ECI **Letmi Ecuador S.A** caduque se realizará un cambio de llaves. La anterior subordinada de ECI y su llave privada solo se usarán para la firma de la CRL mientras existan certificados activos emitidos por la subordinada ECI anterior. Se generará una subordinada ECI **Letmi Ecuador S.A** con una llave privada nueva y un nuevo DN. La llave pública se publicará en el mismo repositorio con un nombre nuevo que la diferencia de la anterior.

5.7 Compromiso y Recuperación ante Desastres.

5.7.1 Procedimientos de gestión de incidentes y compromisos

La ECI **Letmi Ecuador S.A** tiene establecido y probado un **Procedimiento de incidentes de Seguridad de la Información** que establece las acciones a seguir en caso de producirse una vulnerabilidad o un incidente de seguridad. Una vez ejecutados de manera satisfactoria los procedimientos de restablecimiento de los sistemas, se dará servicio al público.

5.7.2 Procedimiento en caso de daño de los recursos informáticos, el software y/o los datos.

En el caso de presentarse una alteración en los recursos de hardware, software o datos se activará el plan de recuperación de desastres (DRP). Se realizará una identificación de la causa de la alteración y se remediará el incidente.

5.7.3 Procedimientos de compromiso de la clave privada de la entidad.

La ECI **Letmi Ecuador S.A** tiene establecido y probado un Plan de Continuidad de Negocio que define las acciones a seguir en caso de producirse una vulnerabilidad de la llave privada de la raíz de la ECI **Letmi Ecuador S.A** o de una de sus subordinadas. En estos casos se deben revocar de manera inmediata las llaves privadas comprometidas de la ECI **Letmi Ecuador S.A** y los certificados firmados bajo su jerarquía. Se debe generar una nueva llave privada y a solicitud de los suscriptores y/ responsables se deben emitir nuevos certificados, adicionalmente, este plan se ejecutará bajo los siguientes escenarios:

1. Cuando el sistema de seguridad de la entidad de certificación ha sido vulnerado.
2. Cuando se presenten fallas en el sistema de la entidad de certificación que comprometan la prestación del servicio.
3. Cuando los sistemas de cifrado pierdan vigencia por no ofrecer el nivel de seguridad contratado por el suscriptor.
4. Cuando se presente cualquier otro evento o incidente de seguridad de la información.

En caso de compromiso de la ECI **Letmi Ecuador S.A**:

1. Aplicar la contención del incidente para prevenir que vuelva a ocurrir
2. Informará a todos los suscriptores, Responsables, Tercero que confía y otras AC con los cuales tenga acuerdos u otro tipo de relación del compromiso.
3. Indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave no son válidos.
    a. Informará a los clientes.

5.7.4 Capacidad de recuperación en caso de desastre.

ECI **Letmi Ecuador S.A** ante un desastre natural u otro tipo de catástrofe, está en capacidad de recuperar los servicios más críticos del negocio, descritos en los documentos asociados a continuidad de negocio, dentro de las cuarenta y ocho (48) horas posteriores a la ocurrencia del evento o dentro del RTO del proceso. El restablecimiento de otros servicios como la emisión de certificados digitales se hará entre los cinco (5) días después de la ocurrencia del evento o según el RPO especificado en el documento de plan de Continuidad de negocio.

5.8 Cese de la CA o la RA.

Procedimiento en caso de cese de la CA y la RA

Antes de su finalización, la AC informará a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con por lo menos treinta (30) días calendario de anticipación. Mientras que, al ARCOTEL, se le informará con por lo menos sesenta (60) días calendario de anticipación.

Todas las solicitudes y contratos de suscriptores y titulares serán transferidos al ARCOTEL o a otro Prestador de Servicios de Certificación designado por éste.

6. CONTROLES TÉCNICOS DE SEGURIDAD.

6.1 Generación e Instalación de Pares de Claves.

6.1.1 Generación de pares de claves

De la ECI Raíz.

La generación del par de llaves de la ECI Raíz, se realizó en las instalaciones del proveedor de servicios de plataforma con las más estrictas medidas de seguridad y bajo el protocolo de ceremonia de generación de llaves establecido para este tipo de eventos y en presencia de un delegado de la ECI. Para el almacenamiento de la llave privada se utilizó un dispositivo criptográfico homologado FIPS 140-2 nivel 3.

De las subordinadas de ECI Letmi Ecuador S.A.

La generación del par de llaves de las subordinadas de ECI **Letmi Ecuador S.A**, se realizó en las instalaciones del proveedor de servicios de ECI **Letmi Ecuador S.A** bajo el protocolo de ceremonia de generación de llaves. Para el almacenamiento de la llave privada subordinada se utiliza un dispositivo criptográfico homologado FIPS 140-2 nivel 3.

De los suscriptores o responsables de ECI Letmi Ecuador S.A.

La generación del par de llaves de los suscriptores de ECI **Letmi Ecuador S.A** , se realiza en las instalaciones del proveedor de servicios de ECI **Letmi Ecuador S.A**. Para el almacenamiento de la llave privada del suscriptor se utiliza un dispositivo criptográfico homologado FIPS 140-2 nivel 3.

6.1.2 Entrega de la clave privada al suscriptor.

La llave privada es entregada al suscriptor y/o responsable en su dispositivo criptográfico y no es posible la extracción de esta. No existe por tanto ninguna copia de llave privada del suscriptor.

6.1.3 Entrega de la clave pública al emisor del certificado.

La llave pública es enviada a la ECI **Letmi Ecuador S.A** como parte de la petición de solicitud del certificado digital.

6.1.4 Entrega de la clave pública de la AC a las partes que confían.

La llave pública de la ECD Raíz y de la ECI Subordinada está incluida en su certificado digital.

Los certificados de la ECD Raíz pueden ser consultados por los terceros que confían en los repositorios listados en el numeral 2.1 Repositorios, Certificados Raíz ***ECI LETMI ECUADOR S.A.***

Los certificados de la ECI Subordinada pueden ser consultados por los terceros de confianza en los repositorios listados en el numeral 2.1 Repositorios, Certificados Subordinadas ECI **Letmi Ecuador S.A**.

6.1.5 Tamaño de las Claves.

Para RSA se tienen definidos los siguientes tamaños de las llaves:

- ECI Raíz de ***ECI LETMI ECUADOR S.A CA*** es de 4096 bits.
- Subordinadas de ECI **Letmi Ecuador S.A** es de 4096 bits.
- Certificados emitidos por ECI **Letmi Ecuador S.A** a usuarios finales es de 2048 bits.

Al intentar derivar la llave privada, a partir de la llave pública de 2048 bits contenida en los certificados de usuarios finales, el problema radica, en encontrar los factores primos de dos números grandes, ya que se tendrían 22047 posibilidades por cada número. Se estima que descifrar una llave pública de 2048 bits requeriría un trabajo de procesamiento del orden de 3 ×1020 MIPS-año*.

- MIPS-año: unidad utilizada para medir la capacidad de procesamiento de un computador funcionando durante un año. Equivale al número de millones de instrucciones que es capaz de procesar un computador por segundo durante un año.

6.1.6 Generación de parámetros de clave pública y control de calidad.

La llave pública de la ECI Raíz está codificada de acuerdo con el estándar RFC 5280 y PKCS#11. El algoritmo de firma utilizado en la generación de las llaves es el RSA o EC.

La llave pública de las subordinadas de ECI **Letmi Ecuador S.A** está codificada de acuerdo con el estándar RFC 5280 y PKCS#11. El algoritmo de firma utilizado en la generación de las llaves es el RSA o EC.

La llave pública de los certificados de usuario final está codificada de acuerdo con el estándar RFC 5280 y PKCS#11. El algoritmo de firma utilizado en la generación de las llaves es el RSA o EC.

La AC genera pares de claves de acuerdo con FIPS 186 y utiliza técnicas razonables para validar la idoneidad de las claves públicas presentadas por el suscriptor. Las claves débiles conocidas se prueban y rechazan en el momento del envío.

6.1.7 Fines de uso de la clave (según el campo de uso de la clave X.509 v3).

Los usos permitidos de la llave para cada tipo de certificado vienen establecidos por las Políticas de Certificado para certificados digitales y en las políticas definidas para cada tipo de certificado emitido por ECI **Letmi Ecuador S.A**.

Todos los certificados digitales emitidos por ECI **Letmi Ecuador S.A** contienen la extensión '*Key Usage'* definida por el estándar X.509 v3, la cual es calificada como crítica.

TIPO DE CERTIFICADO ENTIDAD FINAL - KEY USAGE

Firma Digital -Digital Signature

No Repudio - Non Repudiation

Cifrado de Llave - Key Encipherment

6.2 Protección de clave privada y controles de ingeniería de módulos criptográficos.

6.2.1 Estándares y controles de los módulos criptográficos.

Los módulos criptográficos utilizados en la creación de llaves utilizadas por ECD Raíz de Autoridad de Certificación ***ECI LETMI ECUADOR S.A CA*** cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad.

6.2.2 Control multipersona (m de n) de la clave privada.

Las llaves privadas, de la ***ECI LETMI ECUADOR S.A CA*** Raíz y las llaves privadas de las subordinadas de ECI **Letmi Ecuador S.A**, se encuentran bajo control multipersona.

El método de activación de las llaves privadas es mediante la inicialización del software de ECI **Letmi Ecuador S.A** por medio de una combinación de claves en poder de varias personas

6.2.3 Custodia de la clave privada.

Las llaves privadas de ECI **Letmi Ecuador S.A** se encuentran almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad.

Los datos técnicos del dispositivo son los siguientes:

- **SafeNet Luna SA**

La llave privada de los certificados digitales de usuario final está bajo el exclusivo control y custodia del suscriptor o responsable. En ninguna circunstancia ECI **Letmi Ecuador S.A** guarda copia de la llave privada del suscriptor o certificado administrado por el responsable ya que esta es generada por el mismo suscriptor o responsable y no es posible tener acceso a ella por ECI **Letmi Ecuador S.A**.

6.2.4 Copia de respaldo de la clave privada.

Las llaves privadas de la ECI **Letmi Ecuador S.A** se encuentran almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad. (ver 6.2.3 Custodia de la clave privada**).**

Las copias de backup de las llaves privadas de la ECI **Letmi Ecuador S.A**, están almacenadas en dispositivos externos protegidas criptográficamente por un control dual y solo son recuperables dentro de un dispositivo igual al que se generaron.

6.2.5 Archivo de la clave privada.

Las llaves privadas de ECI **Letmi Ecuador S.A** se encuentran almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad. (ver 6.2.3 Custodia de la llave privada**).**

Las mismas se encuentran en una caja de backups criptográfica en un sitio distinto del lugar en donde se encuentren los HSM.

6.2.6 Transferencia de clave privada o desde un módulo criptográfico.

Las claves privadas se crean de manera directa en los módulos criptográficos utilizados en la producción de Letmi Ecuador S.A.

6.2.7 Método de activación de la clave privada.

Las llaves privadas, de la ECI **Letmi Ecuador S.A** Raíz y de las ECI Subordinadas, se encuentran bajo control multipersona. El método de activación de la llave privada es mediante la inicialización del software de la ECI por medio de una combinación de claves en poder de varios operadores.

Se requiere un control multipersona para la activación de la llave privada de la ECI **Letmi Ecuador S.A**. Se necesitan al menos 2 personas para la activación de las llaves.

6.2.8 Método de desactivación de la clave privada.

La desactivación de la llave privada se realiza mediante desactivación del software o el apagado del servidor ECI. Se activa nuevamente mediante el uso de control multipersona, siguiendo los procedimientos marcados por el fabricante del módulo criptográfico.

6.2.9 Método de destrucción de la clave privada.

El método utilizado en caso de requerirse la destrucción de la llave privada es mediante el borrado de las llaves almacenadas en los dispositivos criptográficos tal y como se describe en el manual del fabricante del dispositivo y la destrucción física de las tarjetas de acceso en poder de los operadores en el caso en el que se requiera.

6.2.10 Clasificación del módulo criptográfico.

Véase sección 6.2.1.

Evaluación del módulo criptográfico.

El dispositivo criptográfico es monitoreado mediante el software propio del mismo para prever posibles fallas.

Evaluación del sistema de cifrado.

ECI **Letmi Ecuador S.A** acoge las recomendaciones para el uso de algoritmos criptográficos y longitudes de clave que sean publicados por el NIST (Instituto Nacional de Estándares y Tecnología por sus siglas en ingles), si se materializa alguna circunstancia en donde los algoritmos utilizados para firma y cifrado por ECI **Letmi Ecuador S.A** sea vean comprometidos a todos los niveles, ECI **Letmi Ecuador S.A.**

6.3 Otros aspectos de la gestión de pares de claves.

6.3.1 Archivo de la clave pública.

ECI **Letmi Ecuador S.A** mantendrá controles para el archivo de su propia llave pública.

6.3.2 Periodos operativos de los certificados y periodos de uso de los pares de claves.

El periodo de uso del par de llaves está determinado por la siguiente vigencia de cada certificado:

Algoritmo RSA:

El periodo de validez del certificado digital de RSA y el par de llaves de la raíz es de treinta (30) años.

El periodo de validez del certificado digital de RSA y el par de llaves de la subordinada es de diez (10) años.

6.4 Datos de Activación.

6.4.1 Generación e instalación de los datos de activación.

Para el funcionamiento de la ECI **Letmi Ecuador S.A** se crean contraseñas para los operadores del dispositivo criptográfico y que servirán junto con un PIN para la activación de las llaves privadas.

Los datos de activación de la llave privada se encuentran divididos en contraseñas custodiadas por un sistema multipersona donde 4 personas comparten el código de acceso de dichas tarjetas.

6.4.2 Protección de los datos de activación.

El conocimiento de los datos de activación es personal e intransferible. Cada uno de los intervinientes es responsable por su custodia y debe manejarlo como información confidencial.

6.4.3 Otros aspectos de los datos de activación.

La clave de activación es confidencial, personal e intransferible y por tanto se deben tener en cuenta las normas de seguridad para su custodia y uso.

6.5 Controles de Seguridad Informática.

Se utilizan sistemas confiables para proporcionar los servicios de certificación, y con el objetivo de garantizar su eficacia, se han implementado controles y auditorías informáticas. Estas acciones aseguran una gestión adecuada de los activos informáticos, alineada con el nivel de seguridad necesario para la administración de sistemas de certificación electrónica.

En cuanto a la seguridad de la información, la Infraestructura de Clave Pública aplica los controles establecidos por el esquema de certificación basado en los sistemas de gestión de la información ISO 27001. Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas, en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Control de accesos a los dispositivos.
- Cierre de vulnerabilidades de los sistemas.
- Hardenización de los sistemas según buenas prácticas.
- Configuración de red a nivel de seguridad (Red Interna, Red administrativa, entre otros)
- Configuración de Usuarios y permisos.
- Configuración de eventos de Log.
- Plan de backup y recuperación.
- Configuración antivirus.
- Requerimientos de tráfico de red configurados en el firewall.

6.5.1 Requisitos técnicos específicos de seguridad informática.

ECI **Letmi Ecuador S.A** cuenta con una infraestructura tecnológica debidamente monitoreada y equipada con elementos de seguridad requeridos para garantizar la disponibilidad y confianza en los servicios ofrecidos a sus suscriptores, entidades y terceros que confían.

La información relacionada con Seguridad de la Información es considerada como confidencial y por tanto solo puede ser suministrada a aquellos entes de control que requieran de su conocimiento.

6.5.2 Clasificación de la seguridad informática.

La seguridad de los equipos de usuario final se gestiona desde ECI **Letmi Ecuador S.A** y se soporta con un análisis de riesgos de tal forma que las medidas de seguridad implantadas sean respuestas a la probabilidad e impacto producido por un grupo de amenazas definidas que puedan aprovechar las brechas de seguridad.

Adicionalmente, se realizan pruebas de seguridad (ethical hacking) periódicas, de manera que se identifiquen posibles vulnerabilidades de los sistemas y que coadyuven con el cierre de estas.

Acciones en caso de un evento o incidente de seguridad de la información.

El sistema de gestión de la seguridad de la Información implementado por ECI **Letmi Ecuador S.A** tiene establecido un procedimiento de gestión de incidentes que especifica las acciones a ejecutar, componentes o recursos a utilizar y como debe reaccionar el personal en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación digital de ECI **Letmi Ecuador S.A**.

1. **Detección y reporte del incidente:** Los incidentes de seguridad deberán ser reportados a través del correo info@letmi.app, el cual es administrado por el Sistema Integrado de Gestión de la ECI **Letmi Ecuador S.A**

Los incidentes podrán ser detectados a través de sistemas de monitorización, sistemas de detección de intrusos, registros del sistema, aviso por parte del personal o por parte de suscriptores y/o responsables.

1. **Análisis y evaluación del incidente:** Una vez detectado el incidente se determina el procedimiento de respuesta y se contacta con las personas responsables para evaluar y documentar las acciones a tomar según la gravedad de la incidencia. Se efectúa una investigación para determinar cuál fue el alcance del incidente, es decir averiguar hasta donde llego el ataque y la máxima información posible de la incidencia.
2. **Control de daños ocasionados por incidente:** Reaccionar rápidamente para contener la incidencia y evitar que se propague tomando medidas como bloquear accesos al sistema.
3. **Investigación y recopilación de evidencias:** Revisar registros de auditoría para realizar un seguimiento de lo ocurrido.
4. **Recuperación y medidas contra incidencia:** Restaurar el sistema a su correcto funcionamiento y documentar el procedimiento y formas de evitar que vuelva a presentarse la incidencia.
5. **Análisis posterior de la incidencia para la mejorar del procedimiento:** Realizar un análisis de todo lo ocurrido, detectar la causa de la incidencia, corregir la causa para el futuro, analizar la respuesta y corregir errores en la respuesta.

6.6 Controles Técnicos del Ciclo de Vida.

6.6.1 Controles de desarrollo del sistema.

ECI **Letmi Ecuador S.A** cumple con los procedimientos de control de cambios establecidos para los nuevos desarrollos y actualizaciones de software.

6.6.2 Controles de gestión de seguridad.

ECI **Letmi Ecuador S.A** mantiene un control sobre los inventarios de los activos utilizados en su proceso de certificación. Existe una clasificación de estos de conformidad con su nivel de riesgo.

ECI **Letmi Ecuador S.A** monitorea de manera periódica su capacidad técnica con el fin de garantizar una infraestructura con la disponibilidad mínima.

6.6.3 Controles de seguridad del ciclo de vida.

ECI **Letmi Ecuador S.A** cuenta con los debidos controles de seguridad a lo largo de todo el ciclo de vida de los sistemas que tengan algún impacto en la seguridad de los certificados digitales emitidos.

6.7 Controles de Seguridad de la Red.

ECI **Letmi Ecuador S.A** cuenta con una infraestructura de red debidamente monitoreada y equipada con elementos de seguridad requeridos para garantizar la disponibilidad y confianza en los servicios ofrecidos a sus suscriptores, entidades y terceros de confianza.

La información relacionada con Seguridad de la Información es considerada como confidencial y por tanto solo puede ser suministrada a aquellos entes de control que requieran de su conocimiento.

El plan de continuidad del negocio de Letmi Ecuador S.A., establece lineamientos y estrategias para asegurar la continuidad y recuperación de productos y servicios en caso de fallos, desastres o eventos que afecten la operación crítica, protegiendo la confidencialidad, integridad y disponibilidad de la información.

Escenarios de Recuperación

Se consideran varios escenarios para la recuperación:

- **Afectación de instalaciones físicas:** Alternativas como sitios de trabajo remoto, transporte alternativo o sedes de emergencia.
- **Caída de sistemas tecnológicos:** Recuperación de hardware y software, incluyendo sistemas críticos y comunicaciones.
- **Ausencia de colaboradores críticos:** Backup de personal identificado.
- **Falta de personal para atención al cliente:** Redistribución de personal de otras áreas.
- **Fallo de proveedores externos:** Garantizar contratos con planes de continuidad y proveedores alternos.

Elementos del Plan de Continuidad

- **Análisis de Impacto al Negocio (BIA):** Identifica procesos y sistemas críticos, evaluando el impacto de interrupciones.
- **Identificación de riesgos:** Análisis de amenazas y vulnerabilidades que afectan la continuidad.
- **Estrategia de continuidad:** Define las acciones para restablecer operaciones.
- **Pruebas:** Se realizan pruebas anuales para evaluar la efectividad del plan.
- **Mantenimiento:** Revisión y actualización periódica del plan.

6.8 Sellado de Tiempo.

ECI **Letmi Ecuador S.A** cuenta con el servicio de sellado de tiempo, que se describe en las correspondientes Políticas de Certificado para Servicio Sellado de Tiempo, publicada en el portal https://letmi.app/

Todos los componentes de la AC se sincronizan periódicamente con un servicio de tiempo fiable. La AC utiliza una fuente de GPS y tres relojes de fuente NTP no autenticados para establecer la hora correcta para:

- Tiempo de validez inicial de un Certificado de AC
- Cancelación de un Certificado de AC.
- Publicación de actualizaciones de CRL; y
- Emisión de Certificados de entidad final de suscriptor. Se pueden usar procedimientos electrónicos o manuales para mantener la hora del sistema. Los ajustes del reloj son eventos auditables.

7. PERFILES DE CERTIFICADO, CRL Y OCSP.

7.1 Perfil del Certificado.

Los certificados cumplen con el estándar X.509 vigente y para la infraestructura de autenticación se basa en el RFC5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

Contenido de los certificados. Un certificado emitido por ECI **Letmi Ecuador S.A**, además de estar firmado digitalmente por ésta, contendrá como mínimo lo siguiente:

1. Nombre, dirección y domicilio del suscriptor.
2. Una Identificación única del suscriptor nombrado en el certificado.
3. El nombre y el lugar donde realiza actividades la AC
4. Llave pública del certificado.
5. La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
6. El número de serie (único) del certificado.
7. Fecha de emisión y expiración del certificado.

Campo	**Valor o restricciones** **RSA (Certificados Entidad Final)**
Versión	3 (0x2)
Número de Serie	Identificador único emitido por ECI Letmi Ecuador S.A
Algoritmo de Firma	SHA256withRSAEncryption
Emisor	Ver sección “Reglas para la interpretación de varias formas de nombre”. Para ECI Letmi Ecuador S.A como emisor se especifica: C = EC L = QUITO O = LETMI ECUADOR S.A. Organization Identifier = VATEC-1793221101001 OU = CA RSA SUB (Certification Services) CN = LETMI RSA SUB C1
Válido desde	Especifica la fecha y hora a partir de la cual el certificado es válido.
Válido hasta	Especifica la fecha y hora a partir de la cual el certificado deja de ser válido.
Sujeto	Conforme a la política del Anexo 1 y las *“Reglas para la interpretación de varias formas de nombre”.*
Llave pública del Sujeto	Codificado de acuerdo con la RFC 5280. Los certificados emitidos por ECI Letmi Ecuador S.A tienen una longitud de 2048 bits y algoritmo RSA.
Identificador de llave de la autoridad	Es utilizado para identificar el certificado emisor en la jerarquía de certificación. Normalmente referencia el campo “Subject Key

	Identifier" de ECI Letmi Ecuador S.A como entidad emisora de certificación digital.
Identificador de la llave del sujeto	Es usado para identificar un certificado que contiene una determinada llave pública.
Directivas del Certificado	Describe las políticas aplicables al certificado, especifica el OID y la dirección URL donde se encuentra disponible las políticas de certificación.
Uso de la llave	Especifica los usos permitidos de la llave. Es un CAMPO CRÍTICO.
Punto de distribución de la CRL	Es usado para indicar las direcciones donde se encuentra publicada la CRL de ECI Letmi Ecuador S.A. En el certificado de la ECI Raíz, este atributo no se especifica.
Acceso a la información de la Autoridad	Es usado para indicar las direcciones donde se encuentra el certificado Emisor de *ECI LETMI ECUADOR S.A CA* Además, para indicar la dirección para acceder al servicio de OCSP.
Nombre alternativo del sujeto	Es usado para indicar la dirección de correo electrónico y adicionalmente para indicar el código acreditación asignado por el ARCOTEL. Nombre RFC822=correo@empresa.com Dirección URL= info@letmi.app
Usos extendidos de la llave	Se especifican otros propósitos adicionales al uso de la llave.
Restricciones básicas	La extensión "PathLenConstraint" indica el número de sub-niveles que se admiten en la ruta del certificado. No existe restricción para ECI Letmi Ecuador S.A, por tanto, es cero.

DATOS CAPTURADOS EN LA SOLICITUD								
	Sello Electrónico -SE (DSCF)	Sello Electrónico -SE (En Archivo)	Persona Natural - PN (DSCF)	Persona Natural - PN (En Archivo)	Representante Legal - RL (DSCF)	Representante Legal - RL (En Archivo)	Miembro Empresa o Empleado con Relación de Dependencia (DSCF)	Miembro Empresa o Empleado con Relación de Dependencia (En Archivo)
Número de identificación solicitante IDC"Indicativo País" - (# Cédula) PAS"Indicativo País" - (# Pasaporte) Ejemplo: IDCEC-1716151413 o PASEC-A6362611			Serial number (SN)	Serial number (SN)	Serial number (SN)	Serial number (SN)	Serial number (SN)	Serial number (SN)
Nombres y apellidos del suscriptor			Common Name (CN)	Common Name (CN)	Common Name (CN)	Common Name (CN)	Common Name (CN)	Common Name (CN)
Apellidos del suscriptor (Solicitante)	Surname	Surname	Surname	Surname	Surname	Surname	Surname	Surname
Nombres del suscriptor (Solicitante)	Given Name (givenName)	Given Name (givenName)	Given Name (givenName)	Given Name (givenName)	Given Name (givenName)	Given Name (givenName)	Given Name (givenName)	Given Name (givenName)
País domicilio del suscriptor			Country (C)	Country (C)				
Localidad (Ciudad) domicilio del suscriptor			Locality (L)	Locality (L)				
Nombre del título o puesto (cargo) del suscriptor. *No es Obligatorio*			Title (T)	Title (T)				
Email del suscriptor (Solicitante)	RFC 822 Name (e-mail address)	RFC 822 Name (e-mail address)	RFC 822 Name (e-mail address)	RFC 822 Name (e-mail address)	RFC 822 Name (e-mail address)	RFC 822 Name (e-mail address)	RFC 822 Name (e-mail address)	RFC 822 Name (e-mail address)
Localidad (Ciudad) domicilio empresa	Locality (L)	Locality (L)			Locality (L)	Locality (L)	Locality (L)	Locality (L)
País domicilio empresa	Country (C)	Country (C)			Country (C)	Country (C)	Country (C)	Country (C)
Nombre completo de la entidad (Empresa) con razón social	Organization (O)	Organization (O)			Organization (O)	Organization (O)	Organization (O)	Organization (O)
Nombre del título o puesto (cargo) del suscriptor ocupado en la empresa					Title (T)	Title (T)	Title (T)	Title (T)
Unidad organizacional de la empresa. *No es Obligatorio*	Organizational Unit Name (OU)	Organizational Unit Name (OU)					Organizational Unit Name (OU)	Organizational Unit Name (OU)
Numero de registro Único de Contribuyente de la empresa	Serial number (SN)	Serial number (SN)						
Descripción uso certificado - Ejemplo (Recepción documentos ventanilla)	Common Name (CN)	Common Name (CN)						

7.1.1 Números de versión.

Los certificados emitidos por ECI **Letmi Ecuador S.A** cumplen con el estándar X.509 vigente.

7.1.2 Extensiones del certificado.

Key Usage.

El "key usage" es una extensión crítica que indica el uso del certificado de acuerdo con el RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

Extensión de política de certificados.

La extensión de "certificatepolicies" del X.509 vigente es el identificador del objeto de esta DPC de acuerdo con la sección identificador de objeto de la Política de Certificación de esta DPC. La extensión no es considerada como crítica.

Nombre alternativo del sujeto.

La extensión "subjectAltName" es requerida y el uso de esta extensión es "No crítico".

Restricciones básicas.

Para el caso de ECI **Letmi Ecuador S.A** en el campo "PathLenConstraint" de certificado de las subordinadas tiene un valor de 0, para indicar que la ECI **Letmi Ecuador S.A** no permite más sub-niveles en la ruta del certificado. Es un campo crítico.

Uso extendido de la llave.

Esta extensión permite definir otros propósitos adicionales de la llave. Es considerada no crítica. Los propósitos más comunes son:

OID	Descripción	Tipos de Certificados
1.3.6.1.5.5.7.3.2	Autenticación de cliente	Todos los tipos de certificado de entidad final
1.3.6.1.5.5.7.3.4	Protección de correo electrónico	Todos los tipos de certificado de entidad final
1.3.6.1.5.5.7.3.8	Sellado de tiempo	Sellado de tiempo

7.1.3 Identificadores de objetos algorítmicos.

El identificador de objeto del algoritmo de firma es:

1.2.840.113549.1.1.11 SHA256 with RSA Encryption

El identificador de objeto del algoritmo de la clave pública es:

1.2.840.113549.1.1.1 rsaEncryption

El identificador de objeto del algoritmo de la clave pública es:

1.2.840.10045.2.1 id-ecPublicKey

7.1.4 Formas de nombres.

De conformidad con lo especificado en el apartado 3.1.1 **Tipos de nombres** de esta DPC.

7.1.5 Restricciones de nombres.

Los nombres se deben escribir en mayúsculas y sin tildes.

El código del país se asigna de acuerdo con el estándar ISO 3166-1 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países".

Respecto a la codificación de los atributos de los DN de los certificados, siguiendo el estándar RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"), se emplea la codificación UTF8String en todos los atributos, contengan o no caracteres especiales, excepto en los atributos en los que es obligatorio utilizar la codificación PrintableString (C, Country; Serial Number).

7.1.6 Identificador del objeto de la Política de Certificación.

El identificador de objeto de la Política de certificado correspondiente a cada tipo de certificado es una subclase de la clase definida en el numeral *1.2 Nombre e identificación del documento* de esta DPC, conforme se establece en las Políticas de Certificado para certificados digitales.

7.1.7 Uso de la extensión "Policy Constrains".

No se estipula restricciones de la política.

7.1.8 Sintaxis y semántica de los calificadores de políticas

El calificador de la política está definido en la extensión de "Certificate Policies" y contiene una referencia al URL donde esta publicada la DPC.

7.1.9 Tratamiento semántico para la extensión de políticas de certificados críticos.

No se estipula restricciones de la política.

7.2 Perfil de CRL.

Las CRL´s emitidas por ECI **Letmi Ecuador S.A** cumplen con la RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile V2" y contienen los elementos básicos.

7.2.1 Número(s) de versión

Las CRL´s emitidas por ECI **Letmi Ecuador S.A** cumplen con la RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile V2" y contienen los elementos descritos en el numeral *7.1 Perfil del Certificado* de la presente DPC

7.2.2 CRL y extensiones de entrada CRL

La información sobre el motivo de la revocación de un certificado estará incluida en la CRL, utilizando las extensiones de la CRL y más específicamente en el campo de motivos de revocación (reasonCode).

7.3 Perfil OCSP.

El servicio OCSP cumple con lo estipulado en el RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

7.3.1 Número(s) de versión

Cumple con la OCSP Versión 1 del RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP" y RFC6019 "The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments".

7.3.2 Extensiones OCSP

Las singleExtensions de una respuesta OCSP NO CONTIENEN la extensión de entrada CRL reasonCode (OID 2.5.29.21).

8. AUDITORIA DE CUMPLIMIENTO Y OTRAS EVALUACIONES.

La ECI **Letmi Ecuador S.A** se encuentra sometida a las revisiones de control de ARCOTEL a la que se ha comunicado del inicio de actividades como Entidad de Certificación.

8.1 Frecuencia o Circunstancias de la Evaluación.

El cumplimiento de los controles que garanticen la seguridad en la emisión de certificados digitales se evaluará por medio de una auditoría anual realizada por una firma de auditoría externa.

8.2 Identidad y cualificaciones del evaluador.

El Comité de Gerencia de la Autoridad de Certificación (AC) podrá delegar las actividades de control en auditores internos o externos, garantizando en todo momento su independencia funcional respecto de las áreas objeto de auditoría. Asimismo, cuando dichas labores sean realizadas por una entidad evaluadora o de inspección, la entidad evaluadora o de inspección debe ser debidamente acreditada por el organismo nacional de acreditación competente y recocido por la autoridad de control., asegurando así la idoneidad, imparcialidad y validez de los procesos de evaluación.

8.3 Relación del evaluador con la entidad evaluada.

La única relación establecida entre el auditor y la entidad auditada es la de auditor y auditado. La firma de auditoría ejerce su absoluta independencia en el cumplimiento de sus actividades de auditoría y no existe conflicto de intereses pues la relación es netamente de tipo contractual.

8.4 Temas cubiertos por la evaluación.

El alcance de la auditoría de conformidad incluye:

- Políticas y practicas
- Conformidad de la DPC con las políticas publicadas
- Gestión del ciclo de vida de claves de la AC
- Gestión del ciclo de vida del certificado
- Sellado de tiempo
- Gestión y operación
- Controles de seguridad y acceso
- Sistema de seguridad de la información
- Gestión de incidentes
- Evaluaciones y análisis de riesgos
- Recopilación de evidencias
- Gestión de la continuidad del negocio
- Planes de Cesación de actividades de la ECI

8.5 Acciones tomadas como resultado de la deficiencia.

Las deficiencias detectadas durante el proceso de auditoría deben ser subsanadas a través de acciones correctivas o de mejora, procedimientos e implementación de los controles requeridos para atender los hallazgos.

8.6 Comunicación de Resultados.

Una vez concluida la auditoría, la firma auditora deberá presentar el informe correspondiente a ECI Letmi Ecuador S.A. Con base en los resultados y, de ser necesario, ECI Letmi Ecuador S.A deberá definir e implementar las acciones correctivas y de mejora pertinentes, orientadas a subsanar los hallazgos identificados y fortalecer continuamente sus procesos.

Así mismo la ECI Letmi Ecuador S.A. deberá presentar a la entidad de acreditación ARCOTEL dentro de los primeros quince (15) días del año siguiente al periodo objeto de evaluación dicho informe de auditoría, en cumplimiento de lo establecido en la Resolución 0176 de 2024.

9. OTROS ASUNTOS COMERCIALES Y LEGALES.

9.1 Honorarios.

No Aplica.

9.1.1 Tasas de emisión de certificados

Letmi Ecuador S.A cobra tasas por la emisión de certificados. **Letmi Ecuador S.A** podrá modificar sus tarifas de conformidad con el contrato de cliente aplicable.

Tarifas de emisión o renovación de certificados.

Detalle del Producto	Vigencia	Precio
Certificados digitales para persona natural	Mensual	**$10** USD +IVA
	1 Año	**$14** USD+IVA
	2 Años	**$25** USD+IVA
Certificados digitales para sello electrónico	Mensual	**$10** USD +IVA
	1 Año	**$14** USD+IVA
	2 Años	**$25** USD+IVA
Certificados digitales para representante legal	Mensual	**$10** USD +IVA
	1 Año	**$14** USD+IVA
	2 Años	**$25** USD+IVA
Certificados digitales para miembro empresa o en relación de dependencia	Mensual	**$10** USD +IVA
	1 Año	**$14** USD+IVA
	2 Años	**$25** USD+IVA

Detalle del Producto	Cantidad de Sellado de Tiempo	Precio
Sellado de Tiempo	1 a 5mil	**$0,14** USD+IVA
	5.001 a 10mil	**$0,13** USD+IVA
	10.001 a 30mil	**$0,12** USD+IVA
	30.001 a 40mil	**$0,11** USD+IVA
	40.001 a 100mil	**$0,09** USD+IVA
	100.001 a 250mil	**$0,06** USD+IVA
	250.001 a 500mil	**$0,05** USD+IVA
	500.001 a 10millones	**$0,04** USD+IVA

Las tarifas de emisión de certificados se encuentra disponible en la página web de **Letmi Ecuador S.A.** https://letmi.app/ .

En este contexto, se establece expresamente que el servicio de consulta de certificados digitales es de carácter gratuito y no genera ningún costo para el usuario.

Para servicios de revocación de certificados **Letmi Ecuador S.A** no cobra tasas por revocación de certificados ni por comprobar el estado de validez de un certificado emitido utilizando una CRL. **Letmi Ecuador S.A** puede cobrar una tasa por proporcionar información sobre el estado de los certificados a través de OCSP

9.1.2 Tasas de acceso a certificados

Si no se especifica en los correspondientes acuerdos legales o CP de un tercero asociado, **Letmi Ecuador S.A** podrá cobrar una tarifa razonable por el acceso a sus bases de datos de certificados, no obstante, el acceso a la consulta del estado de los certificados emitidos es libre y gratuito y por tanto no aplica una tarifa.

9.1.3 Tasas de acceso a información sobre revocación o estado

Letmi Ecuador S.A no cobra tasas por revocación de certificados ni por comprobar el estado de validez de un certificado emitido utilizando una CRL. **Letmi Ecuador S.A** puede cobrar una tasa por proporcionar información sobre el estado de los certificados a través de OCSP

9.1.4 Tasas por otros servicios

Una vez se ofrezcan otros servicios por parte de **Letmi Ecuador S.A**, se encuentran publicadas en la página web de **Letmi Ecuador S.A**. https://letmi.app/

9.1.5 Políticas de Reembolso

Según lo establecido en el correspondiente acuerdo de cliente con Letmi Ecuador S.A.

9.2 Responsabilidad Financiera.

9.2.1 Cobertura del seguro.

La ECI **Letmi Ecuador S.A** mantiene una garantía de responsabilidad civil, de conformidad con lo dispuesto en el apartado h) del artículo 30 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, las Entidades de Certificación de Información y, Servicios Relacionados Acreditadas deberán contar con una garantía de responsabilidad para asegurar a los usuarios el pago de los daños y perjuicios ocasionados por el incumplimiento de las obligaciones..

9.2.2 Otros activos.

Sin estipulación.

9.2.3 Cobertura de seguro o garantía para entidades finales

Sin estipulación.

9.3 Confidencialidad de la Información Comercial.

9.3.1 Alcance de la información confidencial.

ECI **Letmi Ecuador S.A** se compromete a proteger todos los datos a los que tenga acceso como consecuencia de su actividad como ECI.

Toda información no pública es considerada confidencial y por tanto de acceso restringida, excepto en aquellos supuestos previstos legalmente como lo son tribunales u órganos administrativos competentes o impuesta por una ley, no se difunde información confidencial sin el consentimiento expreso por escrito del suscriptor o la entidad que le haya otorgado el carácter de confidencialidad.

No obstante, se reserva el derecho a revelar a los empleados y consultores, externos o internos, los datos confidenciales necesarios para realizar sus actividades como ECI obligando a todo el personal a suscribir un acuerdo de confidencialidad en el marco de las obligaciones contractuales contraídas con ECI **Letmi Ecuador S.A**.

Información confidencial.

La siguiente información es considerada confidencial:

1. Llave privada de la Autoridad de Certificación y/o ECI
2. Llave privada del suscriptor o entidad
3. Información suministrada por el suscriptor o entidad y que no sea necesaria para validar la confianza del suscriptor o entidad
4. Información acerca del solicitante, suscriptor y/o responsable obtenida en fuentes diferentes (por ejemplo, de un reclamante o de los reguladores)
5. Registros de las transacciones
6. Registros de auditoría
7. Políticas de seguridad
8. Plan de Continuidad de Negocio
9. Toda aquella información que sea calificada como "Confidencial" en los documentos entregados por ECI **Letmi Ecuador S.A.**

9.3.2 Información no confidencial.

Toda información no confidencial es considerada pública y por tanto de libre acceso para terceros:

1. La contenida en la presente Declaración de Prácticas de Certificación y sus anexos.
2. La contenida en el repositorio sobre el estado de los certificados.
3. La lista de certificados revocados.
4. Toda aquella información que sea calificada como "PÚBLICA" en los documentos entregados por ECI **Letmi Ecuador S.A**.

9.3.3 Responsabilidad de proteger la información confidencial.

ECI **Letmi Ecuador S.A** mantiene medidas de seguridad para proteger toda la información confidencial suministrada a ECI **Letmi Ecuador S.A** directamente o a través de los canales establecidos para ello desde su recibo hasta su almacenamiento y custodia, donde reposarán de acuerdo a lo definido en la TRD. ECI **Letmi Ecuador S.A** cuenta con un Sistema Integrado de Gestión que incluye un Sistema de Seguridad de la Información. Esto nos permite asegurar que la información de nuestros suscriptores no será comprometida, ni divulgada a terceras personas salvo que medie solicitud formal de una autoridad competente que así la requiera.

9.4 Privacidad de la Información Personal.

Letmi Ecuador S.A. garantiza la protección de los datos personales de los titulares en cumplimiento de la normativa vigente en materia de protección de datos personales. En este sentido, reconoce y asegura el ejercicio de los derechos del titular, conforme a la Ley Orgánica de Protección de Datos Personales (LOPDP), incluyendo de manera expresa:

- **El derecho de acceso**, que permite conocer y obtener información sobre sus datos personales tratados.
- **El derecho de rectificación**, que faculta solicitar la corrección de datos inexactos o incompletos.
- **El derecho de supresión**, que permite solicitar la eliminación de sus datos personales cuando estos no sean necesarios para las finalidades para las cuales fueron recopilados, salvo las excepciones legales aplicables.

El titular podrá ejercer estos derechos mediante solicitud dirigida a Letmi Ecuador S.A., a través de los canales establecidos por la organización que se detallan en la página web https://letmi.app/contacto/ o en esta DPC, los cuales deberán atenderse dentro de los plazos definidos por la normativa vigente.

En relación con la conservación de la información, Letmi Ecuador S.A. mantendrá los datos personales únicamente durante el tiempo necesario para cumplir con las finalidades del tratamiento, así como para atender obligaciones legales, regulatorias y contractuales. En particular, los datos asociados a certificados digitales serán conservados durante la vigencia del certificado y, una vez expirado o revocado, se mantendrán por un período adicional de 10 años, conforme a los requisitos legales, regulatorios y de auditoría aplicables. Finalizado este periodo, la información será eliminada o anonimizada de manera segura.

Letmi Ecuador S.A. implementa medidas técnicas, organizativas y administrativas adecuadas para garantizar la confidencialidad, integridad y disponibilidad de la información personal, evitando su acceso, uso o divulgación no autorizada.

9.4.1 Plan de Privacidad.

La información confidencial se protege mediante medidas de seguridad que garantizan su protección frente a alteración, pérdida, destrucción, daño, falsificación o procesamiento ilícito, de acuerdo a lo dispuesto en el presente documento y en la normativa de referencia aplicable.

9.4.2 Información tratada como privada.

La información personal suministrada por el suscriptor o responsable y que es requerida para la aprobación del certificado digital es considerada información de carácter privado.

9.4.3 Información que no se considera privada.

Son aquellos datos personales que las normas y la Constitución han determinado expresamente como públicos para cuya recolección y tratamiento no es necesaria la autorización del titular de la información.

9.4.4 Responsabilidad de proteger la información privada.

ECI **Letmi Ecuador S.A** es responsable y cuenta con los adecuados recursos tecnológicos, para ayudar a garantizar la adecuada custodia y conservación de los datos de carácter personal recolectados por los canales usados por la compañía, dando cumplimiento a la Ley de Comercio Electrónico, firmas y mensajes de datos. **Letmi Ecuador S.A** ECI hace uso de mecanismos tecnológicos como el directorio activo donde se instrumentaliza la política de control de acceso y un repositorio centralizado donde se encuentra la información protegida por un firewall que previene intrusiones dentro de la red para los equipos de la oficina, y por certificados digitales para el acceso a los servidores de producción de la ECI.

9.4.5 Aviso y consentimiento para utilizar información privada.

Los datos de carácter personal no podrán ser comunicados a terceros, sin la debida notificación y consentimiento de su titular, de conformidad con la normativa aplicable en materia de protección de datos personales.

9.4.6 Divulgación en virtud de un procedimiento judicial o administrativo.

Los datos de carácter personal podrán ser comunicados cuando se requieran por parte de una de las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial sin la debida notificación y consentimiento de su dueño, de conformidad con la normativa de protección de datos personales vigente.

9.4.7 Otras circunstancias de divulgación de información.

Sistema de seguridad para proteger la información.

Respecto al sistema que alberga la información suministrada por el suscriptor o responsable del servicio de certificación se realizan las siguientes validaciones:

1. El proveedor de la infraestructura debe contar con las buenas prácticas de las siguientes Normas:
    a. ISO 27001
    b. ISO 9001
2. Pruebas de penetración y escaneo de vulnerabilidades en la red, realizada por una empresa especializada en Ethical Hacking.

9.5 Derechos de Propiedad Intelectual.

La ECI **Letmi Ecuador S.A** garantiza el cumplimiento de la normativa vigente en cada momento en materia de protección de datos personales, documentando en la presente Declaración de Practicas de Certificación, todos los aspectos, procesos y procedimientos de seguridad correspondientes respecto de los datos de los usuarios. Los datos de los usuarios serán usados única y exclusivamente para los fines indicados frente a cualquier riesgo, amenaza o vulnerabilidad en el presente documento. No se procederá a la divulgación o cesión de los datos personales salvo en los casos previstos en esta DPC.

9.6 Representaciones y Garantías.

En caso de que la ECI Letmi Ecuador S.A no cumpla con las obligaciones a su cargo, los usuarios tendrán a su disposición una garantía de responsabilidad la cual se encuentra a favor de la Secretaria Nacional de Telecomunicaciones para asegurar a los usuarios el pago de los daños y perjuicios ocasionados por lo establecido en este numeral por un monto de cuatrocientos mil dolares de los Estados Unidos (USD $400.000), según los daños o perjuicios que demuestre cada usuario se determinará el monto que se deberá pagar a cada usuario sin que se supere el monto máximo asegurado entre todos los usuarios. Para ello las partes deberán realizar lo que se anuncia en el numeral 9 del documento términos y condiciones.

9.6.1 Declaraciones y garantías de la AC

Salvo que se indique expresamente en la presente DPC o en un acuerdo independiente con un suscriptor, **Letmi Ecuador S.A** no hace ninguna declaración relativa a sus productos o servicios, del mismo modo**,** declara en la medida especificada en esta DPC que cumple en todos los aspectos materiales, con la PC, la presente DPC y todas las leyes aplicables, **Letmi Ecuador S.A** publica y actualiza regularmente la CRL y la base de datos para generar respuestas OCSP.

9.6.2 Declaraciones y garantías de la AR

La AR declara que:

1. Los servicios de emisión y gestión de certificados de la AR se ajustan a la PC de **Letmi Ecuador S.A** y a esta DPC,
2. La información proporcionada por la AR no contiene ninguna información falsa o engañosa,
3. Las traducciones realizadas por la AR son una traducción exacta de la información original, y
4. Todos los certificados solicitados por la AR cumplen con los requisitos de esta DPC.

El acuerdo de **Letmi Ecuador S.A** con la AR puede contener declaraciones adicionales.

Los Acuerdos del suscriptor pueden incluir declaraciones y garantías adicionales.

9.6.3 Declaraciones y garantías del suscriptor

Antes de que se le expida y reciba un Certificado, el suscriptor será el único responsable de cualquier declaración falsa que realice a terceros y de todas las transacciones en las que se utilice la llave Privada del suscriptor, independientemente de que dicho uso haya sido autorizado o no. Los suscriptores están obligados a notificar a **Letmi Ecuador S.A** si se produce un cambio que pueda afectar al estado del Certificado o la solicitud.

Los suscriptores se comprometen a cumplir los compromisos y garantías de esta DPC y a los siguientes puntos:

1. Facilitar información precisa y completa cuando se comunique con **Letmi Ecuador S.A**,
2. Confirmar la exactitud de los datos del certificado antes de utilizarlo,
3. Inmediatamente si aplica:

(i) solicitar la revocación de un Certificado, dejar de utilizarlo y su llave Privada asociada, y notificar a **Letmi Ecuador S.A** si se produce o se sospecha que se ha producido un uso indebido o se ha puesto en peligro la llave Privada asociada a la clave pública incluida en el certificado, y

(ii) solicitar la revocación del Certificado, y dejar de utilizarlo, si cualquier información en el Certificado es o se convierte en incorrecta o inexacta,

1. Garantizar que las personas que utilicen certificados en nombre de una organización hayan recibido la formación de seguridad adecuada y relativa al Certificado,
2. Utilizar el certificado únicamente para fines autorizados y legales, de conformidad con la finalidad del certificado, la presente DPC, cualquier PC aplicable y el correspondiente acuerdo de suscriptor, incluida la instalación de certificados únicamente en servidores autorizados con el consentimiento del suscriptor, y dejar de utilizar inmediatamente el certificado y la llave privada relacionada tras la expiración del certificado.

Los acuerdos de suscripción pueden incluir declaraciones y garantías adicionales.

9.6.4 Declaraciones y garantías de la parte que confía

Cada Parte que confía declara que, antes de confiar en un Certificado emitido por **Letmi Ecuador S.A**:

1. Obtuvo conocimientos suficientes sobre el uso de Certificados digitales y PKI,
2. Ha estudiado las limitaciones aplicables al uso de Certificados y acepta las limitaciones de responsabilidad de **Letmi Ecuador S.A** relacionadas con el uso de Certificados,
3. Ha leído, comprende y acepta el Acuerdo de Parte que confía de **Letmi Ecuador S.A** y la presente DPC,

4. Ha verificado tanto los certificados de suscriptor emitidos por **Letmi Ecuador S.A** como los certificados de la cadena de certificación utilizando la CRL u OCSP correspondiente,
5. No utilizará un certificado emitido por **Letmi Ecuador S.A** si el certificado ha caducado o ha sido revocado, y
6. Adoptará todas las medidas razonables para minimizar el riesgo asociado a la confianza en una firma digital, incluida la confianza únicamente en un certificado emitido por **Letmi Ecuador S.A** después de considerar:

a) la legislación aplicable y los requisitos legales para la identificación de las partes, la protección de la confidencialidad o privacidad de la información, y la aplicabilidad de la transacción;

b) el uso previsto del Certificado tal y como se enumera en el certificado o en esta DPC,

c) los datos enumerados en el Certificado

d) el valor económico de la transacción o comunicación

e) la pérdida o el daño potencial que causaría una identificación errónea o una pérdida de confidencialidad o privacidad de la información en la solicitud, transacción o comunicación,

f) la trayectoria anterior de la Parte que Confía en el suscriptor,

g) los conocimientos comerciales de la parte que confía, incluida la experiencia con métodos comerciales informáticos, y

h) cualquier otro indicio de fiabilidad en relación con el suscriptor y/o la aplicación, comunicación o transacción.

Toda confianza no autorizada en un Certificado es por cuenta y riesgo de la parte que confía.

Los Acuerdos de Parte que confía pueden incluir declaraciones y garantías adicionales.

9.6.5 Declaraciones y garantías de otros participantes

No Aplica

9.7 Renuncias de Garantías.

No Aplica

9.8 Límites de Responsabilidad.

De acuerdo con lo establecido en la norma de Arcotel Resolución 0176 de 2024, la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y en el Reglamento de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos , Letmi Ecuador S.A. ha suscrito una póliza de seguro con una entidad aseguradora autorizada de acuerdo con la legislación ecuatoriana, que ampara los perjuicios contractuales y extracontractuales de los suscriptores y terceros de buena fe exenta de culpa derivados de errores y omisiones o de actos de mala fe de los administradores, representantes legales o empleados de Letmi en el desarrollo de sus actividades.

La cuantía asegurada es de $400.000 USD.

Letmi Ecuador S.A., en su calidad de entidad de certificación, asegura que la emisión y administración de los certificados de firma electrónica se efectúa conforme a lo dispuesto en su Declaración de Prácticas de Certificación (DPC) y en la Política de Certificación (PC) aplicable. En consecuencia, no asumirá responsabilidad por los perjuicios que puedan derivarse del uso de dichos certificados por parte de los suscriptores o de terceros, siempre que su actuación se haya realizado en estricto cumplimiento de dichas disposiciones. Sin perjuicio de lo anterior, Letmi Ecuador S.A. responderá por los daños directos que se generen como resultado de incumplimientos atribuibles a su gestión, siempre que los suscriptores o terceros hayan observado íntegramente lo establecido en la DPC y la PC. En todos los casos, la responsabilidad de la entidad se limitará a los daños efectivamente comprobados, excluyéndose cualquier tipo de daño indirecto, incidental, consecuencial o especial, cualquiera sea su naturaleza. Asimismo, los valores de reposición o compensación aplicables en caso de dichos daños estarán sujetos a las tarifas vigentes publicadas en la página web de Letmi Ecuador S.A. y a las establecidas en el numeral 9.1.1 “Tasas de emisión de certificados”.

Las condiciones específicas de la póliza se relacionan a continuación, conforme a lo establecido en el documento:

- AMPARO O COBERTURA BÁSICA
  La presente póliza cubre el riesgo de incumplimiento del contrato y para responder por las obligaciones que contrajere el Contratista a favor de terceros, relacionados con el contrato.
  En los contraltos de obra, así como en los contratos integrales por precio fijo, esta póliza garantizará también la debida ejecución de la obra y la buena calidad de los materiales, asegurando con ello las reparaciones o cambios de aquellas partes de la obra en la que se descubran defectos de construcción, mala calidad o incumplimiento de las especificaciones, imputables al proveedor. La Compañía no responderá por el incumplimiento del contrato que sea ocasionado por fuerza mayor o caso fortuito debidamente comprobados. Con cargo a esta garantía se podrán efectivizar las multas que le fueren impuestas al contratista, hasta su valor asegurado.
- EXCLUSIONES GENERALES
  Esté póliza no cubrirá incumplimiento del Afianzado relacionados con:
  a) Clausulas penales, indemnizaciones civiles, laborales o administrativas derivadas del contrato afianzado;
  b) Pago de intereses de cualquier tipo generados por el contrato afianzado por esta póliza; salvo estipulaciones legales en contrario.
  c) Obligaciones de otros contratos celebrados entre el Afianzado y el Asegurado, que no sean los garantizados en esta Póliza; o que no hubieren sido comunicados a la Aseguradora .
  Adicionalmente esta póliza no cubrirá el incumplimiento del Afianzado que sean ocasionados a causa de fuerza mayor o caso fortuito debidamente comprobado .
- DOCUMENTOS NECESARIOS PARA LA RECLAMACIÓN DE SINIESTROS
  Para reclamar el pago de esta póliza, se requerirá presentar a la Compañía la resolución administrativa suscrita por la máxima autoridad de la Entidad Asegurada o su delegado, en la que se declare el incumplimiento del contrato, o la mora del Contratista en sus obligaciones frente a terceros, incluso cuando el cobra de la póliza sea por concepto de las multas impuestas al Contratista. Recibida dicha resolución acompañada de los informes técnicos y económicos, referente al cumplimiento de las obligaciones de la Entidad Contratante y del Contratista, la Compañía procederá al pago del valor Asegurado en caso de incumplimiento de contrato o al pago del valor requerido para satisfacer obligaciones del contratista frente a terceros. En todo caso, se adjuntará al reclamo los documentos que acrediten el Incumplimiento de la obligación afianzada y la cuantía del perjuicio ocasionado.
- PAGO DE LA INDEMNIZACIÓN
  Una vez recibida por la Compañía el pedido por escrito del Asegurado de la ejecución de la póliza y la documentación detallada en el articulo anterior, la Compañía procederá sin más trámites al pago de la suma asegurada, dentro del plazo que determine la Ley. El Asegurado no podrá iniciar ninguna demanda, acción o proceso judicial contra la Compañía, en virtud de esta póliza, durante este periodo. Si el Asegurado al momento de ejecutar la póliza, fuere deudor del Afianzado por cualquier concepto, al momento de pagarse la indemnización se compensará el monto de dicha deuda. La Compañía al pagar cualquier indemnización por concepto esta póliza, quedará relevada de toda responsabilidad para con el asegurado.

La indemnización a que da derecho esta póliza podrá ser cobrada únicamente por el Asegurado, o por el delegado que se designe por escrito. En caso de que la Compañía resuelva pagar la indemnización, tal pago se hará a través de transferencias o medios de pago electrónicos a la cuenta designada para tal efecto por el Asegurado dentro de los diez (10) días siguientes al que el Asegurado o sus representantes presentaron por escrito la reclamación, aparejada de los documentos estipulados en el presente contrato.

Responsabilidad por la veracidad de la información del suscriptor.

El suscriptor asume todos los riesgos por perjuicios que pudieran derivarse de conductas como otorgar información falsa, suplantar la identidad de terceros, validar documentos o información incompleta o desactualizada.

Responsabilidad por disponibilidad del servicio.

El suscriptor se compromete a obrar diligentemente para reducir al mínimo las posibilidades de fallas o interrupciones que puedan llegar a presentar al interior de su organización. Las fallas ocasionadas por la incapacidad o insuficiencia de los equipos del suscriptor, o por su falta de conocimientos frente al uso del servicio, no serán en ningún caso imputables a ECI **Letmi Ecuador S.A** y no se podrá exigir de su parte el saneamiento de ningún perjuicio.

Responsabilidad por la funcionalidad del servicio en la infraestructura del suscriptor.

El suscriptor será el único responsable de la provisión y el pago de los costos necesarios para asegurar la compatibilidad del servicio (certificado de firma digital), frente a sus equipos, incluyendo todo el hardware, software, componentes eléctricos y otros componentes físicos o lógicos requeridos para acceder y usar el mismo, incluyendo de forma enunciativa pero no limitativa servicios de telecomunicaciones, acceso y conexión a Internet, enlaces, navegadores, u otros programas, equipos y servicios requeridos para acceder y usar el servicio.

Responsabilidad frente delitos informáticos.

En el evento en que el suscriptor sea víctima de alguna de las conductas tipificadas como delito, en sus sistemas de información, en sus aplicaciones e infraestructura tecnológica, en la ejecución de transacciones electrónicas o en el acceso y uso del servicio, ataques de phishing, suplantaciones de identidad, por negligencia en el manejo y confidencialidad del certificado digital, este será el único responsable y saneará los perjuicios a que haya lugar, toda vez que es su obligación adoptar las medidas de seguridad, políticas, campañas culturales, instrumentos legales y demás mecanismos para salvaguardar la confidencialidad y el buen uso de su certificado digital.

Exenciones de responsabilidad de las garantías.

ECI **Letmi Ecuador S.A** no será responsable en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales, terrorismo, huelgas o cualquier otro caso de Fuerza Mayor.
- Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente DPC y sus Anexos.
- Por el uso indebido o fraudulento de los certificados o CRL's emitidos por la Autoridad de Certificación.
- Por el uso de la información contenida en el Certificado o en la CRL.
- Por el incumplimiento de las obligaciones establecidas para el suscriptor, Entidades, Responsables o Terceros que confían en la normativa vigente, la presente DPC y sus Anexos.
- Por el perjuicio causado en el periodo de verificación de las causas de revocación /suspensión.
- Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
- Por la no recuperación de documentos cifrados con la clave pública del suscriptor o Entidad.
- Fraude en la documentación presentada por el solicitante.

9.9 Indemnizaciones.

No Aplica.

9.10 Duración y Terminación.

9.10.1 Duración.

La DPC y PC entran en vigor desde el momento en que se publican en la página web de ECI **Letmi Ecuador S.A**, a partir de ese momento la versión anterior del documento queda derogada y la nueva versión reemplaza íntegramente la versión anterior.

ECI **Letmi Ecuador S.A** conserva en el repositorio las anteriores versiones de la DPC y PC.

9.10.2 Terminación.

Para los certificados digitales que hayan sido emitidos bajo una versión antigua de la DPC o PC aplica la nueva versión de la DPC o PC en todo lo que no se oponga a las declaraciones de la versión anterior.

9.10.3 Efecto de terminación, notificación y comunicación.

ECI **Letmi Ecuador S.A** notifica los cambios en la presente declaración de prácticas de certificación publicando en la página web la nueva versión una vez sea autorizada por el apoderado y en la misma se registrará el control de cambios respectivo.

9.10.4 Procedimiento de Cambio en la DPC y PC.

Cambios que afectan la DPC y PC.

Todo cambio que afecte la DPC y PC de la ECI **Letmi Ecuador S.A** seguirá el siguiente procedimiento:

1. El apoderado aprobará los cambios que considere pertinentes sobre la DPC y las PC.
2. La DPC y PC actualizada es publicada en la página web de la ECI **Letmi Ecuador S.A** una vez sea autorizada por el apoderado.

Circunstancias bajo las cuales la OID debe cambiarse.

En los siguientes casos la ECI **Letmi Ecuador S.A** realizará ajustes a la identificación de OID:

1. La autorización de una nueva jerarquía de certificación, evento en el cual los OID deberán ser definidos de acuerdo con la estructura.
2. En caso de que los cambios de la DPC y PC que afecten la aceptabilidad de los servicios de certificación digital se proceden a realizar el ajuste de OID.

Este tipo de modificaciones se comunicará a los usuarios de los certificados correspondientes a la PC o DPC.

9.11 Notificaciones y comunicaciones individuales a los participantes.

9.11.1 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 y en lo dispuesto en las Políticas de Certificación y en esta DPC a:

1. Respetar lo dispuesto en la normatividad vigente, en esta DPC y en las Políticas de Certificación PC.
2. Publicar esta DPC y cada una de las Políticas de Certificación en la página Web de **Letmi Ecuador S.A**.
3. Mantener la DPC con su última versión publicada en la página Web de **Letmi Ecuador S.A**.
4. Notificar a la ARCOTEL en los tiempos establecidos la ocurrencia de de cualquier evento que comprometa la disponibilidad y la seguridad en la prestación de los servicio de Certificacion de Informacion y Servicios relacionados de la ECI **Letmi Ecuador S.A**. de acuerdo con la RESOLUCIÓN ARCOTEL-2024-0176 del 16 de agosto de 2024
5. Proteger y custodiar de manera segura y responsable su llave privada.
6. Emitir certificados conforme a las Políticas de Certificación y a los estándares definidos en la presente DPC.
7. Generar certificados consistentes con la información suministrada por el solicitante o suscriptor.
8. Conservar la información sobre los certificados digitales emitidos de conformidad con la normatividad vigente.
9. Emitir certificados cuyo contenido mínimo este de conformidad con la normativa vigente para los diferentes tipos de certificados.
10. Publicar el estado de los certificados digitales emitidos en un repositorio de acceso libre.
11. No mantener copia de la llave privada del solicitante o suscriptor.
12. Actualizar y publicar la lista de certificados digitales revocados CRL con los últimos certificados revocados.
13. Informar a los suscriptores la proximidad del vencimiento de su certificado digital.
14. Informar a los suscriptores la proximidad del vencimiento de su certificado digital.

15. Revocar los certificados digitales según lo dispuesto en el procedimiento de revocaciones de certificados digitales.
16. Notificar al Solicitante, Suscriptor o Entidad la revocación del certificado digital dentro de las 24 horas siguientes a la revocación del certificado de conformidad con el procedimiento de revocaciones de certificados digitales.
17. 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**.
18. Proporcionar al solicitante en la página web de la ECI **Letmi Ecuador S.A** la siguiente información de manera gratuita y acceso libre cumpliendo con los parámetros y características de la normatividad vigente sin inducir al error:
    - La Declaración de Prácticas de certificación sus Anexos, las Políticas de Certificado y todas las actualizaciones de los documentos mencionados.
    - Obligaciones del suscriptor y la forma en que han de custodiarse los datos.
    - Procedimiento para solicitar la emisión de certificado.
    - El procedimiento de revocación de su certificado.
    - Las condiciones y límites del uso del certificado
19. 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.
20. Actualizar la información de contacto cada vez que haya cambio o modificación en los datos suministrados.
21. 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.
22. Garantizar la protección, integridad, confidencialidad y seguridad de la información suministrada por el suscriptor conservando la documentación que respalda los certificados emitidos.
23. Garantizar las condiciones de integridad, disponibilidad, confidencialidad y seguridad, de acuerdo con los estándares técnicos nacionales e internacionales vigentes.
24. Disponer en la página web de la ECI **Letmi Ecuador S.A** los servicios que se encuentran acreditados.

9.11.2 Obligaciones de la AR.

La AR de la ECI **Letmi Ecuador S.A** es la encargada de realizar la labor de identificación y registro, por lo tanto, la AR está obligada en los términos definidos en esta Declaración de Prácticas de Certificación a:

1. Conocer y dar cumplimiento a lo dispuesto en la presente DPC y en las Políticas de Certificación 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 suscriptores de certificados digitales.
4. Verificar la exactitud y autenticidad de la información suministrada por el Solicitante.
5. Archivar y custodiar la información y/o documentación suministrada por el solicitante o suscriptor 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 suscriptor.
7. Identificar e informar a la ECI **Letmi Ecuador S.A** las causas de revocación suministradas por los solicitantes sobre los certificados digitales vigentes.

9.11.3 Obligaciones (Deberes y Derechos) del suscriptor y/o Responsable.

El suscriptor como suscriptor o responsable de un certificado digital está obligado a cumplir con lo dispuesto por la normativa vigente y lo dispuesto en la presente DPC como es:

1. Usar su certificado digital según los términos de esta 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 **Letmi Ecuador S.A**.
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 solicitud o utilizando los canales, medios o mecanismos dispuestos por **Letmi Ecuador S.A** para la solicitud de certificados digitales para facilitar su oportuna y plena identificación.
6. Solicitar la revocación del certificado digital ante el cambio de nombre y/o apellidos.
7. Solicitar la revocación del certificado digital cuando el suscriptor haya variado su nacionalidad.
8. Cumplir con lo aceptado y/o firmado en el documento términos y condiciones.
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 las PC establecidos en la presente DPC para cada uno de los tipos de certificado.
13. Solicitar como suscriptor y/o responsable de manera inmediata la revocación de su certificado digital cuando tenga conocimiento que existe una causal definida en numeral *Circunstancias para la revocación de un certificado* de la presente DPC.
14. No hacer uso de la llave privada ni del certificado digital una vez cumplida su vigencia o se encuentre revocado.
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 el estado de un certificado digital revocado para lo cual se 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** que pueda considerar engañosa o no autorizada, conforme a lo dispuesto por esta DPC y PC.
19. Una vez caducado o revocado el servicio de certificación digital el suscriptor debe inmediatamente dejar de utilizarla en todo el material publicitario que contenga alguna referencia al servicio.
20. El suscriptor 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 esta DPC, indicando la versión.
21. El suscriptor 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. Solicitar información referente a las solicitudes en proceso.
3. Solicitar revocación del certificado digital aportando la documentación necesaria.

9.11.4 Obligaciones de los Terceros que confían.

Los Terceros que confían 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.
3. Verificar el estado de los certificados digitales 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.

9.11.5 Obligaciones de la Entidad (Cliente).

Conforme lo establecido en las PC relacionadas en este documento, en el caso de los certificados donde se acredite la vinculación del suscriptor y/o responsable con la misma, será obligación de la Entidad:

1. Solicitar a la AR de la ECI **Letmi Ecuador S.A** la suspensión/revocación del certificado digital 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 relacionadas en esta 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.

9.11.6 Obligaciones de otros participantes de la ECI.

El Comité de Gerencia y el 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 los cambios a realizar sobre los servicios de certificación, por decisiones de tipo normativo o por solicitudes de suscriptor o responsables.
3. Aprobar la notificación de cualquier cambio a los suscriptores y/o responsables analizando su impacto legal, técnico o comercial.
4. Revisar y tomar acciones sobre cualquier comentario realizado por suscriptor o responsables cuando un cambio en el servicio de certificación 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 revocación de un certificado digital si tuviera el conocimiento o sospecha del compromiso de la llave privada del suscriptor, entidad o cualquier otro hecho que tienda al uso indebido de llave privada del suscriptor, 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 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 por que las condiciones de acreditación otorgadas por el organismo competente se mantengan.
16. El Sistema Integrado de Gestión ejecutará planes de acción correctivos y acciones de mejora para responder ante cualquier riesgo que comprometa la imparcialidad 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 y no discriminación de la ECI, entregando a el apoderado el mecanismo que elimina o minimiza tal riesgo, de manera continua.
17. 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 que comprometan su imparcialidad.
18. Documentar y demostrar el compromiso de imparcialidad y no discriminación.
19. 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 esta ECI.
20. 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.

9.12 Enmiendas.

Los certificados digitales emitidos por ECI **Letmi Ecuador S.A** no puede ser modificados, es decir, no aplican enmiendas. En consecuencia, el suscriptor debe solicitar la emisión de un nuevo certificado digital. En este evento se expedirá un nuevo certificado al suscriptor; el costo de esta modificación será asumido completamente por el suscriptor conforme a las tarifas informadas por ECI **Letmi Ecuador S.A** o según las condiciones definidas a nivel contractual.

9.12.1 Procedimiento para enmienda.

No aplica ya que los certificados digitales emitidos por ECI **Letmi Ecuador S.A** no pueden ser modificados.

9.12.2 Mecanismo y plazo de notificación.

No aplica ya que los certificados digitales emitidos por ECI **Letmi Ecuador S.A** no pueden ser modificados.

9.12.3 Circunstancias en las que debe modificarse un OID.

No aplica ya que los certificados digitales emitidos por ECI **Letmi Ecuador S.A** no pueden ser modificados.

9.12.4 Notificación al suscriptor o responsable de la emisión de un nuevo certificado.

No aplica ya que los certificados digitales emitidos por ECI **Letmi Ecuador S.A** no pueden ser modificados.

9.12.5 Forma en la que se acepta la modificación de un certificado.

No aplica ya que los certificados digitales emitidos por ECI **Letmi Ecuador S.A** no pueden ser modificados.

9.12.6 Publicación del certificado modificado por la ECI.

No aplica ya que los certificados digitales emitidos por ECI **Letmi Ecuador S.A** no pueden ser modificados.

9.12.7 Notificación de la emisión de un certificado por la ECI a otras entidades.

No aplica ya que los certificados digitales emitidos por ECI **Letmi Ecuador S.A** no pueden ser modificados.

9.13 Disposiciones sobre resolución de disputas.

Si por alguna razón surge alguna diferencia entre las Partes (suscriptor/responsable y ECI **Letmi Ecuador S.A** con ocasión de:

1. La prestación de los servicios de certificación digital descritos en esta DPC.
2. Durante la ejecución de los servicios contratados.
3. Por la interpretación del contrato, DPC y cualquier otro documento entregado por ECI **Letmi Ecuador S.A**.

La parte interesada notificará a la otra parte vía correo electrónico certificado la existencia de dicha diferencia, con la información completa y debidamente sustentada de la diferencia, a fin de que dentro de los quince (15) días hábiles siguientes a dicha notificación, las Partes busquen llegar a un arreglo directo entre ellas como primera instancia.

Finalizado dicho período la(s) diferencia(s) persista(n), las Partes quedaran en la libertad de acudir ante la justicia ordinaria colombiana para hacer valer sus derechos o exigencias, que se sujetará a las normas vigentes sobre la materia, los costos que se causen con ocasión de la convocatoria estarán totalmente a cargo de la Parte vencida.

9.14 Legislación aplicable.

El funcionamiento y las operaciones realizadas por la ECI **Letmi Ecuador S.A**, así como la presente Declaración de Prácticas de Certificación y las Políticas de Certificación aplicables a cada tipo de certificado están sujetas a la normativa que les sea aplicable

9.15 Cumplimiento de la legislación aplicable.

La ECI **Letmi Ecuador S.A** manifiesta el compromiso por cumplir la normativa que les sea aplicable.

9.16 Disposiciones varias.

9.16.1 Acuerdo completo

La ECI **Letmi Ecuador S.A** obliga contractualmente a cada AR a cumplir con esta DPC y las directrices aplicables del sector. Asimismo, la ECI **Letmi Ecuador S.A** exige que cada parte que utilice sus productos y servicios celebre un acuerdo en el que se definan las condiciones asociadas al producto o servicio. Si un acuerdo contiene disposiciones que difieren de la presente DPC, prevalecerá la presente DPC. Los terceros no podrán basarse en dicho acuerdo ni emprender acciones para exigir su cumplimiento, si dicho acuerdo es contrario a la presente DPC.

9.16.2 Cesión

Las entidades que operen en virtud de esta DPC no podrán ceder sus derechos u obligaciones sin el consentimiento previo por escrito de la ECI **Letmi Ecuador S.A**.

9.16.3 Divisibilidad

Si alguna disposición de la presente DPC es declarada inválida o inaplicable por un juzgado o tribunal competente, el resto de la DPC seguirá siendo válida y aplicable.

9.16.4 Ejecución (honorarios de abogados y renuncia de derechos)

La ECI **Letmi Ecuador S.A** puede solicitar indemnización y honorarios de abogados a cualquiera de las partes por daños, pérdidas y gastos relacionados con la conducta de dicha parte.

El hecho de que la ECI **Letmi Ecuador S.A** no haga cumplir una disposición de esta DPC no implica que renuncie a su derecho de hacer cumplir la misma disposición más adelante o a su derecho de hacer cumplir cualquier otra disposición de esta DPC.

Para ser efectivas, las renuncias deberán constar por escrito y estar firmadas por la ECI **Letmi Ecuador S.A**.

9.16.5 Fuerza mayor

La ECI **Letmi Ecuador S.A** no será responsable de ningún retraso o incumplimiento de una obligación en virtud de la presente DPC en la medida en que el retraso o incumplimiento se deba a un hecho ajeno al control razonable de la ECI **Letmi Ecuador S.A**.

El funcionamiento de Internet escapa al control razonable de la ECI **Letmi Ecuador S.A**.

En la medida en que lo permita la legislación aplicable, los Contratos de suscriptor y los Contratos de Parte que confía incluirán una cláusula de fuerza mayor que proteja a la ECI **Letmi Ecuador S.A**.

9.17 Otras Disposiciones.

CAMBIOS QUE AFECTEN LOS SERVICIOS DE CERTIFICACIÓN DIGITAL.

ECI **Letmi Ecuador S.A** puede realizar ajustes o cambios a los servicios de certificación digital en los siguientes eventos:

1. Por cambios normativos en la legislación para ECI.
2. Cambios tecnológicos que afecten los servicios de certificación digital.
3. Por solicitud de suscriptores o responsables, previa aprobación del apoderado.

Para lo cual el suscriptor o responsable deberá enviar comunicación dirigida a el apoderado de la ECI **Letmi Ecuador S.A** sobre el cambio solicitado, la aceptación o rechazo estará bajo la discreción del apoderado.

Procedimiento para los Cambios.

Cambios que no requieren notificación.

Cuando los cambios realizados no afecten el funcionamiento de los servicios prestados a los suscriptores o responsables actuales, será labor del comité de Gerencia definir el nivel de impacto de los cambios.

Cuanto los cambios impliquen correcciones tipográficas o de edición en el contenido de los servicios prestados.

Cambios que requieren notificación

Cuando los cambios realizados afecten el funcionamiento de los servicios prestados a los suscriptores o responsables actuales, será labor del comité de Gerencia definir el nivel de impacto de los cambios.

Cuando los cambios impliquen actualización de datos de contacto con la ECI Letmi Ecuador S.A.

Mecanismo y periodo de notificación

ECI **Letmi Ecuador S.A** notificará por correo electrónico y/o portal web, a los suscriptores, responsables, con la información técnica detallada y las modificaciones a contratos, sobre el cambio realizado a los servicios de certificación digital, cuando:

1. El Comité de Gerencia y el proceso del Sistema Integrado de Gestión de la ECI **Letmi Ecuador S.A** considere que los cambios a los servicios de certificación digital afectan el funcionamiento y aceptabilidad de estos.
2. Los cambios introduzcan nuevos requisitos para la prestación de los servicios de certificación digital por actualizaciones tecnológicas o cambios normativos que afecten los servicios.

Los suscriptores y/o responsables de los servicios de certificación digital afectados por los cambios realizados pueden presentar sus comentarios o rechazo a la prestación del servicio de la ECI **Letmi Ecuador S.A** en comunicación dirigida a el comité de Gerencia dentro de los treinta (30) días siguientes a la notificación, pasados los treinta (30) días se entenderá como aceptadas las condiciones por parte de los suscriptores o responsables.

DESCRIPCIÓN DE PRODUCTOS Y SERVICIOS

TIPO DE CERTIFICADO DIGITAL	OBJETO

Certificado de firma digital Persona Natural	Son certificados que identifican al suscriptor como una persona natural y será responsable a título personal de todo lo que firme electrónicamente, dentro del ámbito de su actividad y límites de uso que correspondan.
Certificado de firma digital Sello Electrónico	Son certificados que identifican al suscriptor como una persona jurídica de derecho público o privado a través de su representante legal o de las personas que actúen en su representación, quien es serán responsables en tal calidad de todo lo que firmen dentro del ámbito de su competencia y límites de uso que correspondan.
Certificado de firma digital Representante Legal	Es un mensaje de datos que identifica al representante legal o apoderado que será el signatario y su vinculación con la persona jurídica pública o privada que es el titular de la firma.
Certificado de Miembro empresa o en Relación de Dependencia	Son certificados que tienen por objeto acreditar la identidad de la persona natural titular y su vinculación con una persona jurídica en virtud de una relación laboral o contractual, permitiéndole realizar actuaciones y transacciones electrónicas dentro del ámbito de sus funciones, sin que ello implique el otorgamiento de facultades adicionales a las propias de su cargo.
Sellado de tiempo (TSA)	Mensaje de datos que vincula a otro mensaje de datos con un momento o periodo de tiempo concreto, el cual permite establecer con una prueba que estos datos existían en ese momento o periodo de tiempo y que no sufrieron ninguna modificación a partir del momento en que se realizó el sellado.

Nota: Para la verificación del proceso de generación de cada servicio remitirse a los procedimientos correspondientes.

POLÍTICAS DE CERTIFICACIÓN.

La interrelación entre esta DPC y la Políticas de certificación de los distintos certificados es fundamental. Y ello, en la medida en que:

- **La DPC** es el conjunto de prácticas adoptadas por ECI **Letmi Ecuador S.A** para la prestación de los servicios acreditados por ARCOTEL y contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los certificados, además sobre la relación de confianza entre Solicitante, suscriptor, Responsable, Entidad, Tercero de buena fe y la ECI.
- **Políticas de certificación** constituye el conjunto de reglas que definen las características de los distintos certificados ECI **Letmi Ecuador S.A** y la aplicabilidad de estos certificados para determinadas aplicaciones que exigen los mismos requisitos de seguridad y formas de usos.

En definitiva, la política define "**qué**" requerimientos son necesarios para la emisión de los distintos certificados ECI **Letmi Ecuador S.A** mientras que la DPC nos dice "**cómo**" se cumplen los requerimientos de seguridad impuestos por la política.

Por este motivo, se relacionan las siguientes Políticas de Certificados:

- Políticas de Certificado para Certificados Digitales Persona Natural en DSCF y en Archivo:

OID (Object Identifier) - IANA	1.3.6.1.4.1.62566.2.1
Ubicación de la PC	https://letmi.app/documentos/Marco_regulatorio/politicas/Politicas_de_Certificado_para_Certificados_Digitales_Persona_Natural_DSCF_y_en_Archivo_V4.pdf

- Políticas de Certificado para Servicio de Certificados Digitales Miembro Empresa o en Relación de Dependencia en DSCF y en Archivo

OID (Object Identifier)	1.3.6.1.4.1.62566.2.2
Ubicación de la PC	https://letmi.app/documentos/Marco_regulatorio/politicas/Politicas_de_Certificado_para_Certificados_Digitales_Miembro_Empresa_o_en_Relacion_de_Dependencia_en_DSCF_y_e

- Políticas de Certificado para Certificados Digitales Representante Legal en DSCF y en Archivo:

OID (Object Identifier) - IANA	1.3.6.1.4.1.62566.2.3
Ubicación de la PC	https://letmi.app/documentos/Marco_regulatorio/politicas/Politicas_de_Certificado_para_Certificados_Digitales_Representante_Legal_DSCF_y_en_Archivo_V4.pdf

- Políticas de Certificado para Certificados Digitales Sello Electrónico en DSCF y en Archivo:

OID (Object Identifier) - IANA	1.3.6.1.4.1.62566.2.4
Ubicación de la PC	https://letmi.app/documentos/Marco_regulatorio/politicas/Politicas_de_Certificado_para_Certificados_Digitales_Sello_Electronico_DSCF_y_en_Archivo_V4.pdf

- Políticas de Certificado para Servicio de Sellado de Tiempo:

OID (Object Identifier) – IANA	1.3.6.1.4.1.62566.2.5
Ubicación de la PC	https://letmi.app/documentos/Marco_regulatorio/politicas/Politica_de_Certificado_para_Sellado_de_Tiempo_V4.pdf

- Políticas de Certificado para Validación OCSP:

OID (Object Identifier) – IANA	1.3.6.1.4.1.62566.2.6.2
Ubicación de la PC	https://letmi.app/documentos/Marco_regulatorio/politicas/Politicas_de_Certificados_de_validación_OCSP_V3.pdf

ANEXO 1 DPC MATRIZ PERFIL TÉCNICO CERTIFICADOS DIGITALES.
ANEXO 2 DPC MODELOS Y MINUTAS DE LOS DOCUMENTOS DE TÉRMINOS Y CONDICIONES.

Firmado electrónicamente por:
CRISTIAN PATRICIO ALVEAR CUARAN
Validar únicamente con FirmaEC

Elaboró

Firmado electrónicamente por:
JONATHAN RAFAEL CUAICAL MARTÍNEZ
Validar únicamente con FirmaEC

Revisó

Firmado electrónicamente por:
LILIANNE MARTINEZ LEDEA
Validar únicamente con FirmaEC

Aprobó

Letmi Ecuador S.A

Consulte el documento firmado