DECLARACIÓN DE POLÍTICAS DE CERTIFICACIÓN (DPC)

Versión 2.1

LAZZATE

Tabla de contenido

1. Introducción

1.1. Presentación

Este documento constituye la Declaración de Prácticas de Certificación (DPC) para la emisión de certificados de LAZZATE CIA. LTDA., en el marco del cumplimiento de los Criterios Específicos de Acreditación Entidades de Certificación de la Información y Servicios Relacionados vigente, establecidos por la Agencia de Regulación y Control de la Telecomunicaciones ARCOTEL, conforme a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su reglamento.

Esta DPC establece las prácticas que lleva a cabo LAZZATE CIA. LTDA. para emitir, gestionar, revocar y renovar certificados digitales, siguiendo el estándar RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", y conforme a los siguientes estándares:

RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
ITU-T X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.
ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
ETSI EN 319 412-2 Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
ETSI EN 319 412-3 Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.
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 LAZZATE CIA. LTDA. 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 LAZZATE CIA. LTDA. 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.

En el caso de que se detecten vulnerabilidades o se pierda la vigencia de los estándares técnicos o infraestructura indicados en la presente DPC, LAZZATE CIA. LTDA. se encargará de informar de tal hecho a la ARCOTEL, para proceder con la respectiva actualización.

Existe una Política de Certificación por cada tipo de certificado emitido y un Texto de Divulgación.

MARCO LEGAL

Base Legal

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su Reglamento; Ley Orgánica de Defensa del consumidor, Ley Orgánica de Transparencia de la Información y Acreditación de ARCOTEL.

Soporte Legal

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el Registro Oficial No. 577 de 17 de abril de 2002.

De conformidad con lo dispuesto en el Art. 37 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, el Consejo Nacional de Telecomunicaciones es el Organismo de autorización, registro y regulación de las Entidades de Certificación de Información y Servicios Relacionados Acreditados.

Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, expedido mediante Decreto Ejecutivo No. 3496 publicado en el Registro Oficial 735 de 31 de diciembre de 2002, y reformas constantes en Decreto Ejecutivo 1356 de 29 de septiembre de 2008, publicadas en el Registro Oficial No. 440 de 6 de octubre de 2008.

El segundo artículo enumerado agregado por el artículo 4 del Decreto Ejecutivo No. 1356 a continuación del artículo 17 del Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, dispone que la acreditación como entidad de certificación de información y servicios relacionados, consistirá en un acto administrativo emitido por el CONATEL a través de una resolución que será inscrita en el Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados.

La Resolución 477-20-CONATEL-2008 de 08 de octubre de 2008, aprueba el modelo de resolución para la Acreditación como Entidad de Certificación de Información y Servicios Relacionados.

Resolución ARCOTEL-CTHB-CTDS-2022-0068 de 10 de mayo de 2022, que acredita a LAZZATE CIA. LTDA. como Entidad de Certificación de Información y Servicios Relacionados, acto que fue inscrito y consta en el Acta 1 Págoina 13 del Libro de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados del Registro Público de Telecomunicaciones, en cumplimiento a lo dispuesto en el artículo 144 de la Ley Orgánica de Telecomunicaciones, la Ley de Comercio Electrónico, Firmas Electrónicas y mensajes de Datos, su Reglamento; y demás disposiciones legales y reglamentarias pertinentes.

1.2. Nombre del documento e identificación

1.2.1. Identificación

Nombre	Declaración de Prácticas de Certificación
Código	LAZZATE-EC-ECU-DPC-01
Versión	1.0
Descripción	Declaración de Prácticas de Certificación de LAZZATE CIA. LTDA.
Fecha de emisión	22/08/2022
Tipo de documento	PÚBLICO
OID	1.3.6.1.4.1.59382.1.1
Localización	http://enext.ec/descargas/politicas/dpc.pdf

1.2.2. OID

Siguiendo los estándares de certificación digital, LAZZATE CIA. LTDA. 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".

1.3. Entidades participantes

1.3.1. Autoridades de Certificación (CA)

LAZZATE forma parte de la Jerarquía de Certificación de que está compuesto por diversas Autoridades de Certificación (en inglés CA o *Certificate Authority*).

Autoridad de Certificación Raíz

La Autoridad de Certificación, es la entidad lógica y de confianza que se encarga de emitir y revocar un Certificado Digital que se utilizarán en la firma electrónica, empleando para ello criptografía de clave pública. Las principales funciones de la CA son:

- Emitir certificados electrónicos.
- Publicar y facilitar el acceso al estado de vigencia de los certificados.
- Garantizar la identidad de los titulares de los certificados.
- Garantizar la veracidad de la información incluida en los certificados.
- Revocar los certificados cuando tiene conocimiento de que se ha puesto en riesgo la seguridad del sistema.
- Administrar la Infraestructura de Clave Pública en conformidad con las normas legales y técnicas vigentes en cada momento.

Autoridades de Certificación Subordinadas

Es la responsable de emitir los certificados para las CA Subordinadas o secundarias a la CA Raíz, las cuales están relacionadas con los terceros vinculados y usuarios finales.

Las Sub CA pueden emitir certificados para personas natural, jurídica y miembro de empresa.

1.3.2. Autoridad de Registro (RA)

La Autoridad de Registro, comprueba y registra la identidad de los certificados digitales de los usuarios y de los terceros vinculados.

En una infraestructura de clave pública, una RA (autoridad de registro) es una entidad de confianza que:

Registra las peticiones que hagan los usuarios para obtener un certificado.

Comprueba la veracidad y corrección de los datos que aportan los usuarios en las peticiones.

Validar la identidad del Suscriptor, del Solicitante, y del Firmante o del Custodio de claves, y comprobar que cumplen con los requisitos necesarios para la solicitud de los certificados.

Validar los atributos de la persona física o jurídica que constarán en el certificado como Firmante o Creador del sello.

Envía las peticiones a una CA (autoridad de certificación) para que sean procesadas.

Podrán actuar como RA de LAZZATE CIA. LTDA.:

- La propia LAZZATE CIA. LTDA. directamente.
- Cualquier empresa / compañía que llegue a un acuerdo con LAZZATE CIA. LTDA. para

la emisión de certificados a nombre de la Corporación o de aquellas personas físicas con las que la Corporación tenga una vinculación, ya sea como empleados, asociados, colaboradores, clientes o proveedores.

- Cualquier Tercer Vinculado que llegue a un acuerdo con LAZZATE CIA. LTDA. para actuar como intermediario en nombre de LAZZATE CIA. LTDA..

LAZZATE CIA. LTDA. formalizará contractualmente las relaciones entre ella y cada una de las empresas o entidades que actúen como RA de LAZZATE CIA. LTDA..

La empresa o entidad que actúe como RA de LAZZATE CIA. LTDA. podrá autorizar a una o varias personas como **Terceros Vinculados** para operar con el sistema informático de emisión de certificados de LAZZATE CIA. LTDA. en nombre de la RA.

1.3.3. Solicitante

Solicitante es la persona natural o jurídica que solicita a LAZZATE CIA. LTDA. la emisión de un certificado.

Los requisitos que debe reunir un Solicitante dependerán del tipo de certificado solicitadoy estarán recogidos en la correspondiente Política de Certificación.

1.3.4. Suscriptor

Suscriptor es la persona natural o jurídica a cuyo nombre el Ente de Certificación LAZZATE CIA. LTDA. expide un certificado digital y, por tanto, actúa como responsable de este, y que, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en esta DPC y en la PC correspondiente y habiendo firmado el respectivo documento de solicitud y aceptación con LAZZATE CIA. LTDA., acepta las condiciones del servicio de emisión de certificados prestado por éste.

El Suscriptor es el responsable del uso de la clave privada asociada al certificado expedido a su nombre por LAZZATE CIA. LTDA., a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando dicha clave privada.

Concretamente:

- En el caso de certificados Personales, el Suscriptor es la persona física titular del certificado.
- En el caso de certificados de Empresa y para la Función Pública, el Suscriptor es la Corporación (empresa, entidad privada o pública) o la Entidad Pública que ha contratado los servicios de certificación de LAZZATE CIA. LTDA.

1.3.5. Custodio de claves

El Custodio de claves es la persona física que posee un dispositivo de creación de firma o sello electrónicos o tiene control sobre el mismo, y que actúa en su nombre yderecho, o bien como sujeto vinculado a una Corporación (empresa, entidad privada o pública) o a una Administración Pública, suscriptor del certificado.

El Custodio de claves será responsable de custodiar los datos de creación de firma o sello electrónicos, es decir, la clave privada asociada al certificado, o los datos de acceso a los mismos, es decir, los datos que permiten utilizar la clave privada asociada al certificado.

Concretamente:

- En el caso de certificados Personales, Corporativos de Persona Física y Corporativos de Firma Empresarial, el Custodio de claves es siempre la persona física titular del certificado, es decir, el Firmante.
- En el caso de certificados Corporativos de Sello Electrónico y de Sello de Administración, órgano o entidad de derecho público, el Custodio de claves es el Solicitante u otra persona física autorizada por el Solicitante para obtener el certificado.

1.3.6. Tercero que confía en los certificados

Se entiende como tercero que confía en los certificados (en inglés, *relaying party*) a toda persona u organización que voluntariamente confía en el certificado de entidad final emitido por LAZZATE CIA. LTDA..

La Autoridad de Certificación LAZZATE CIA. LTDA. está subordinada a la Autoridad de Certificación Raíz del ECIL (Ente de Certificación de la Información LAZZATE), entidad con la que comparte la mayoría de las prácticas de certificación debido al acuerdo de prestación de servicios entre ambas.

1.4. Tipos de certificados de Lazzate Cia. Ltda.

1.4.1. Certificados para Personas Naturales

Certificados para Persona Natural: son certificados que permiten identificar y firmar al Suscriptor como una Persona Natural sin vinculación a ninguna empresa o entidad.

OID DE POLÍTICAS DE CERTIFICADOS PERSONALES

1.3.6.1.4.1.59382.2.1 PC para Persona Natural de LAZZATE CIA. LTDA.

1.4.2. Certificados para Empresas

Certificados para Representante Legal: son certificados que permiten identificar y firmar al Suscriptor como Persona Natural vinculada a una empresa o entidad (Persona Jurídica), como su representante legal.

Certificados para Vinculación a Empresa/Entidad: son certificados que permiten identificar y firmar al Suscriptor como Persona Natural vinculada a una empresa o entidad (Persona Jurídica o Persona Natural), ya sea como empleado, asociado o colaborador.

Certificados para Firma Automatizada: son certificados que permiten identificar y firmar al

Suscriptor como empresa o entidad (Persona Jurídica o Persona Natural), que se emiten para dispositivos informáticos, programas o aplicaciones dedicados a firmar en nombre de la empresa o entidad en sistemas de firma digital automatizada.

1.4.3. Certificados para Función Pública

Certificados para Función Pública: son certificados que permiten identificar y firmar al suscriptor como Persona Natural Vinculada a una empresa o entidad pública (funcionario público).

1.5. Usos no autorizados de los certificados

No se permite el uso que sea contrario a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y sus Reglamento vigentes en el Ecuador. Tampoco se permite la utilización distinta de lo establecido en esta Declaración de Prácticas de Certificación y en su correspondiente Política de Certificación.

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Los certificados de usuario final no pueden emplearse para firmar certificados de clave pública de ningún tipo, ni firmar listas de certificados revocados.

LAZZATE CIA. LTDA. no ofrece el servicio de recuperación de la clave privada, no siendo posible recuperarlos datos cifrados con la correspondiente clave pública en caso de pérdida o inutilización de la clave privada o del dispositivo que la custodia por parte del Suscriptor, o del Firmante o del Custodio de claves. La persona u organización que decida cifrar información lo hará en todo caso bajo su propia y única responsabilidad, sin que, en consecuencia, LAZZATE CIA. LTDA. tengaresponsabilidad alguna por pérdida de información derivada de la pérdida de las claves decifrado. Por ello, LAZZATE CIA. LTDA. no recomienda el uso de los certificados para el cifrado de la información.

1.6 Administración de las políticas

1.6.1. Organización responsable

El Departamento Técnico de LAZZATE CIA. LTDA. es la organización responsable de la administración deesta DPC y de las PC.

1.6.2. Persona de contacto

Organización responsable:	LAZZATE CIA. LTDA.
Persona de contacto:	Director Técnico de LAZZATE CIA. LTDA.

E-mail:	info@lazzatecorp.com
Teléfono:	+593 500 0150
Dirección:	LAZZATE CIA. LTDA. Av. Brasil N39-22 y pasaje N39D

1.6.3. Frecuencia de revisión

Esta DPC y las PC serán revisadas y, si procede, actualizadas anualmente.

1.6.4. Procedimiento de aprobación

Esta DPC y las PC son aprobadas por el Comité de Sistemas de Gestión de LAZZATE CIA. LTDA. antes de ser publicadas, después de que se controlen las versiones de estas, a fin de evitar modificaciones y suplantaciones no autorizadas y el uso de documentación obsoleta.

Las nuevas versiones aprobadas de esta DPC y de las PC serán enviadas al organismo de control y publicadas en la página web de LAZZATE CIA. LTDA. http://enext.ec/descargas/politicas/dpc.pdf Los cambios en cada nueva versión estarán indicados en la tabla inicial de historial de versiones.

1.7. Definiciones y Acrónimos

1.7.1. Definiciones

Algoritmo: conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien deba realizar dicha actividad. Dados un estado inicial y siguiendo los pasos sucesivos se llega a un estado final y se obtiene una solución.

Autoridad de Certificación: Certification Authority (CA). Es una entidad de confianza, responsable de emitir y revocar los certificados digitales, publicación de certificados, publicación de listas de certificados revocados, etc.

Autoridad de Registro: La Autoridad de Registro, comprueba y registra la identidad de los certificados digitales de los usuarios y de los terceros vinculados.

En una infraestructura de clave pública, una RA (autoridad de registro) es una entidad de confianza que:

- Registra las peticiones que hagan los usuarios para obtener un certificado.
- Comprueba la veracidad y corrección de los datos que aportan los usuarios en las peticiones.
- Envía las peticiones a una CA (autoridad de certificación) para que sean procesadas.

Autoridad de sellado de tiempo (TSA): Esta entidad proporciona prueba de tiempo independiente e irrefutable para transacciones, documentos y firmas digitales. Se puede utilizar para crear pruebas de peso legal de que las transacciones ocurrieron en un momento definido en el tiempo, que los documentos electrónicos existieron en un momento particular y que no se han modificado posteriormente. También puede probar de forma independiente cuándo el firmante aplicó una firma digital para que se pueda verificar su validez a largo plazo, incluso después de la expiración o revocación de las credenciales digitales del firmante.

CA Raíz: La Autoridad de Certificación, es la entidad lógica y de confianza que se encarga de emitir y revocar un Certificado Digital que se utilizarán en la firma electrónica, empleando para ello criptografía de clave pública.

CA Subordinada: Es la responsable de emitir los certificados para las CA Subordinadas o secundarias a la CA Raíz, las cuales están relacionadas con los terceros vinculados y usuarios finales.

Clave privada: ver Datos de Creación de Firma.

Clave pública: ver Datos de Verificación de Firma.

Certificado digital: mensaje de datos electrónico firmado por la ECIL, el cual identifica tanto a el ECIL que lo expide, como al suscriptor y contiene la clave pública de este último.

Cliente: en los servicios de certificación digital, el término "cliente" identifica a la persona natural o jurídica con la cual el ENTE DE CERTIFICACIÓN establece una relación comercial.

Datos de Creación de Firma (Clave privada): valores numéricos únicos que, utilizados juntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos.

Datos de Verificación de Firma (Clave pública): datos que son utilizados para verificar que una firma digital fue generada con la clave privada del suscriptor.

Declaración de Prácticas de Certificación (DPC): documento en el que constan de manera detallada los procedimientos que aplica el Ente de Certificación para la prestación de sus servicios. Una declaración de las prácticas que el Ente de Certificación emplea para emitir, gestionar, revocar y renovar certificados sin y con cambio de claves.

Estampado cronológico (Estampa cronológica, Sello de tiempo o Sellado de tiempo, Time stamp o Time stamping en inglés): mensaje de datos firmado digitalmente y con sello de tiempo por una TSA que vincula a otro mensaje de datos con un momento de tiempo concreto, el cual permite establecer con una prueba que estos datos existían en ese momento y que no sufrieron ninguna modificación a partir del momento en que se realizó el estampado.

Firma Centralizada: se llama "firma centralizada" a la gestión centralizada de los certificados digitales, de manera que estos certificados operen desde un repositorio único, controlado y seguro. De manera práctica esto implica que los certificados digitales son generados y almacenados en el servidor, lo que permite que puedan ser usados desde cualquier ordenador o dispositivo móvil.

Firma Digital: se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático reconocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

Función Hash: operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.

HSM Centralizado: dispositivo criptográfico en el cual se genera, almacenan y protegen las claves criptográficas de los suscriptores de una forma segura, permitiendo la firma centralizada o firma en la nube.

Lista de Certificados Digitales Revocados (CRL): aquella relación que debe incluir todos los certificados revocados por la ENTE DE CERTIFICACIÓN.

Log: servicio de registro de eventos del sistema de información, dejando la información anterior y la actual, identifica quién y cuándo se realizó el evento.

Niveles de seguridad: diversos niveles de garantía que ofrecen las variables de firma electrónica cuyos beneficios y riesgos deben ser evaluados por la persona, empresa o institución que piensa optar por una modalidad de firma electrónica para enviar o recibir mensajes de datos o documentos electrónicos.

OID: identificador único de objeto (object identifier). OID. Acrónimo del término en idioma inglés "Object Identifier", que consiste en un número único de identificación asignado en base a estándares internacionales y comúnmente utilizado para identificar documentos, sistemas, equipos, etc., con la finalidad, entre otras cosas, de conocer el origen, la titularidad y la antigüedad del objeto identificado.

PKI: Infraestructura de clave pública (Public Key Infraestructure). Es el conjunto de hardware, software, políticas, procedimientos y elementos tecnológicos que, mediante la utilización de un par de claves criptográficas, una privada que sólo posee el suscriptor del servicio y una pública, que se incluye en el certificado digital, logran:

- Identificar al emisor de un mensaje de datos electrónico.

- Impedir que terceras personas puedan observar los mensajes que se envían a través de medios electrónicos.

- Impedir que un tercero pueda alterar la información que es enviada a través de medios electrónicos.

- Evitar que el suscriptor del servicio de certificación digital que envió un mensaje electrónico pueda después negar dicho envió.

Política de Certificados (PC): conjunto de reglas que indica los requisitos de un certificado en una comunidad y/o clase en particular, en el marco de los requisitos legales, reglamentarios, y con requisitos de seguridad comunes.

Revocación: proceso por el cual se inhabilita el certificado digital emitido y se da por terminado su periodo de validez de uso a partir de la fecha de revocación, al presentarse alguna de las causas establecidas en la Declaración de Prácticas de Certificación.

Servicio de certificación digital: conjunto de actividades certificación que ofrece el Ente de Certificación para certificar el origen e integridad de mensajes de datos, basados en las firmas digitales o electrónicas, estampado de tiempo, así como en la aplicabilidad de estándares técnicos admitidos y vigentes en infraestructura de llave pública – PKI.

Sello de tiempo: ver Estampado cronológico.

Solicitante: persona natural o jurídica que, con el propósito de obtener servicios de certificación digital de una Ente de Certificación, demuestra el cumplimiento de los requisitos establecidos en la DPC y la PC correspondiente para acceder al servicio de certificación digital. Persona natural o jurídica que solicita a el Ente de Certificación la emisión de un certificado.

Suscriptor: persona natural o jurídica a cuyo nombre se expide un certificado digital. Persona natural o jurídica que, habiendo firmado el respectivo documento de solicitud y aceptación, acepta las condiciones del servicio de emisión de certificados prestado por la Ente de Certificación.

Unidad de sellado de tiempo (TSU): conjunto de hardware y software que es gestionado como una unidad y tiene una única clave de firma de sellos de tiempo activa en un instante de tiempo.

a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o

b) la creación, verificación y validación de certificados para la autenticación de sitiosweb, o

c) la preservación de firmas, sellos o certificados electrónicos relativos a estosservicios;

1.7.2. Acrónimos

CA: Autoridad de Certificación. (Certificate Authority)
ACI: Instituto Americano de Concreto (American Concrete Institute).
ACL: Listas de control de acceso (Access Control List).
AdES: Son formatos que cumples con los sets de estándares europeos (Advanced Electronic Signatures).
AFO: Flujo de Aire de Adelante hacia atrás (Front-to-back airflow)
API: Interfaz de programación de apliaciones (Application Programing Interface)
APP: Aplicación Mobil (Application Movil)
ARCOTEL: Agencia de Regulación y Control de las Telecomunicaciones
ARL: Listas de Autoridades de Certificación Revocadas (Authority Revocation List).
ARP: Protocolo de Resolución de Direcciones (Address Resolution Protocol).
ASCE: Sociedad Americana de Ingenieros Civiles (American Society of Civil Engineers)
AV: Autoridad de Validación.

BD: Base de Datos.
BGP: Protocolo de Enlace de Puerta de Frontera (Border Gateway Protocol).
CaasS: Comunicaciones como Servicio (CaaS).
CMP: Protocolo de Administración de Certificados (Certificate Management Protocol)
CMVP: Programa de Validación de Módulos Criptográficos (Cryptographic Module Validation Program).
CRL: Listado de Certificados Revocados (Certificate Revocation List).
CSP: Proveedor de Servicios Criptográficos (Cryptographic Service Provider).
CTI: Centros Tecnológicos Integrados.
DCIM: Infraestructura para la administración de Data Center (Data Center Infraestructure Management)
DHCP: Protocolo de Configuración Dinámica de Host (Dynamic Host Control Protocol).
DPC: Declaración de Prácticas de Certificación.
DRaaS: Servicio de Recuperación ante Desastres (Disaster Recovery as a Service).
DSA: Algoritmo de Firma Digital (Digital Signature Algorithm)
EAL: Niveles de confianza en la evaluación (Evaluation Assurance Level).
EJBCA: Software libre de infraestructura PKI.
ECI: Entidad de Certificación de la Información.
eIDAS: Reglamento Europeo para la Identificación electrónica (electronic IDentification, Authentication and trust Services).
EMC: Compatibilidad Electromagnética (Electromagnetic Compatibility).
EMI: Interferencia Electromagnética (Electromagnetic Interference).
EMSA: Método de Codificación para Firmas con Apéndice (Encoding Method for Signatures with Appendix).
ESP: Carga Útil de Seguridad Encapsulada (Encapsulating Security Payload).
EST: Inscripción sobre Transporte Seguro (Enrollment over Secure Transport).
ETSI: Instituto de Estandares de Telecomunicaciones Europeas (European Telecommunications Standars Institute).
FCC: Comisión Federal de las Comunicaciones (Federal Communications Commission).
FIPS: Estándares Federales de Procesamiento de la Información (Federal Information Processing Standard).
GFS: Secuencia de respaldo (Grandfather-Father-Son).
HA: Alta Disponibilidad (High Availability).
HASH: Algoritmo matemático de función criptográfica
HSM: Módulo de Seguridad de Hardware (Hardware Security Module).
HTTP: Protocolo de transferencia de hipertexto (Hypertext Transfer Protocol o HTTP).
IaaS: Infraestructura como Servicio.
IdP: Proveedor de Identidad (Identity Provider).
IEEE: Instituto de Ingeniería Eléctrica y Electrónica (Institute of Electrical and Electronics Engineers).
IGMP: Protocolo de Administración de Grupos de Internet (Internet Group Management Protocol).
INOCAR: Instituto Oceanográfico de la Armada
IS-IS: Protocolo de Sistema Intermediario a Sistema Intermediario (Intermediate System to Intermediate System).
JSON: Notación de Objetos de JavaScrip (JavaScript Object Notation).
ITU-T: Sector de Estandarización de Telecomunicaciones de la Unión de Telecomunicaciones Internacionales (-Internacional Telecommunication Union- Telecommunication Standardization Sector).
LACP: Protocolo de Control de Agregación de Enlaces (Link Aggregation Control Protocol).
LAG: Grupos de Agregación de Enlaces (Link Aggregation Groups).

LAN: Red de Área Local (Local Area Network).
LDAP: Protocolo de Acceso a Servicios de Directorio (Lightweight Directory Access Protocol).
ND: Protocolo de descubrimiento dispositivo cercano (Neighbor Discovery).
NEBS: Sistema de Construcción de Redes (Network Equipment-Building System).
NEC: Norma Ecuatoriana de Construcción.
NIST: Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology).
NTP: Protocolo en Red de Tiempo (Network Time Protocol)
OCSP: Servicio de Protocolo de Comprobación de un Certificado en Línea (En línea Certificate Status Protocol).
OSPF: Protocolo de Primer Camino más Corto (Open Shortest Path First).
OTP: Pasword de único uso (One Time Pasword).
PKCS: Estándares de Criptografía de Clave Pública (Public-Key Cryptography Standards).
PKI: Infraestructura de Clave Pública (Public Key Infrastructure).
PoE: Alimentación a través de Ethernet (Power Over Ethernet).
PSS: Esquema Probabilístico para Firma (Probabilistic Signature Scheme).
QES: Firma Electrónica Cualificada (Qualified Electronic Signature).
QSCD: Dispositivo de creación de firma electrónica cualificada (Qualified Electronic Signature Creation Device).
RA: Autoridad de Registro. (Register Authority)
RFC: Peticiones de Comentarios (Request For Comments).
RIP: Protocolo de Información de Enrutamiento (Routing Information Protocol).
RPO: Punto Objetivo de Recuperación (Recovery Point Objective).
RSA: Algoritmo Rivest, Shamir, Adleman (Rivest, Shamir, Adleman).
RTO: Tiempo Objetivo de Recuperación (Recovery Time Objective).
SaaS: Software como Servicio.
SAM: Módulo de Activación de Firmas (Signature Activation Module).
SAML: Lenguaje de Marcado para Confirmaciones de Seguridad (Security Assertion Markup Language).
SCEP: Protocolo de Inscripción Simple de Certificados (Simple Certificate Enrollment Protocol).
SFC: Servidor de Firma Centralizada.
SHA: Algoritmo de Hash Seguro (Secure Hash Algorithm).
SLA: Acuerdos de Nivel de Servicio (Service Level Agreement).
SMS: Servicio de Mensajería Corto (Short Message Service).
SOAP: Protocolo de Acceso de Objeto Simple (Simple Object Access Protocol).
SPA: Adaptadores de Puertos Compartidos (Shared Port Adapters).
SSA: Esquema para Firmas con Apéndice (Signature Scheme with Appendix).
SSL: Capa de Sockets Seguros (Secure Sockets Layer).
Sub CA: Autoridad de Certificación Subordinada (Subordinate Certificate Authority)
TCP: Protocolo de Control de Transmisión (Transport Control Protocol).
TDR: Reflectometría por Dominio de Tiempo (Time Domain Reflectometry).
TI: Tecnología de la Información (Technology Information).
TIER: Nivel de fiabilidad de un centro de Datos.
TSA: Autoridad de Sellado de Tiempo (Time Stamp Authority).
UDP: Protocolo de Datagrama del Usuario (User Datagram Protocol).
URL: Localizador de Recursos Uniforme (Uniform Resource Locator)
VA: Autoridad de Validacion (Validation Authotity).
VLAN: Red Virtual de Área Local (Virtual Local Area Network).
VoIP: Voz Sobre Protocolo de Internet (Voice Over Internet Protocol).
VGW: Puerta de enlace Virtual (Virtual Gateway).

WYSIWYS: Lo que se ve es lo que se firma (What You See Is What You Sign).
XML: Lenguaje de Marcado (Extensible Markup Language).

2. Repositorios y publicación de información

2.1. Repositorios

Acceso	Descripción	URL
Público	DPC, Políticas de Certificación, PDS, Condiciones Generales de Contratación	http://enext.ec/descargas/politicas/dpc.pdf
Público	Certificado CA Raíz El ECI LAZZATE CIA. LTDA.	http://enext.site/root.crt
Público	Certificado CA Subordinada LAZZATE CIA. LTDA.	http://enext.site/root.crt
Público	CRL: Lista de Certificados de entidad final Revocados (CRL emitida por CA Subordinada LAZZATE CIA. LTDA.)	http://enext.site/crl/
Público	Servicio de Validación de Certificados de CA (OCSP de CA Raíz	http://enext.site/ocsp/
Público	Servicio de Validación de Certificados de entidad final (OCSP de CA Subordinada LAZZATE CIA. LTDA.)	http://enext.site/ocsp/

Los repositorios están referenciados por la URL. Cualquier cambio en las URL se notificará a todas las entidades que puedan verse afectadas.

Las direcciones IP correspondientes a cada URL podrán ser múltiples y dinámicas, pudiendo ser modificadas sin previo aviso.

La información en las URL estará disponible en línea las 24 horas del día, los 7 días de la semana.

En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de LAZZATE CIA. LTDA., éste realizará los mayores esfuerzos para asegurar que la información en las URL no se encuentre indisponible durante más tiempo que el periodo máximo de 24 horas.

2.2. Publicación de información

2.2.1. Políticas y Prácticas de Certificación

La versión actual de la DPC, las Políticas de Certificación, y las Condiciones Generales de Contratación estarán disponibles en formato electrónico en la Web de LAZZATE CIA. LTDA., www.enext.ec.

LAZZATE CIA. LTDA. mantiene publicadas en su Web las versiones anteriores de la DPC, las Políticas de Certificación y el Texto de Divulgación de PKI (PDS) mientras existan certificados vigentes que se hayan emitido de acuerdo con dichos documentos. Las versiones retiradas de la Web podrán ser solicitadas por los interesados en la dirección de contacto de LAZZATE CIA. LTDA.

2.2.2. Términos y condiciones

La relación contractual entre LAZZATE CIA. LTDA. y los Suscriptores está basada en la firma del documento de Solicitud y Aceptación del Servicio que corresponda, y la aceptación de la Declaración de Prácticas de Certificación, las PC que correspondan y las Condiciones Generales de Contratación de LAZZATE CIA. LTDA. publicadas en su página web, www.enext.ec.

2.2.3. Difusión de los certificados

El Firmante o el Creador del sello será el responsable de hacer llegar su certificado a todo aquel tercero que desee autenticar a un usuario o comprobar la validez de una firma electrónica. Este envío se realizará generalmente de manera automática, adjuntando el certificado a todo documento firmado o sellado electrónicamente.

2.3. Frecuencia de publicación

Según la Declaración de Prácticas de Certificación de El ECI LAZZATE CIA. LTDA., la CA Raíz emitirá y publicará una Lista de Certificados de CA Revocados (ARL) como mínimo cada seis meses, o extraordinariamente, cuando se produzca la revocación de un certificado de Autoridad de Certificación Subordinada.

LAZZATE CIA. LTDA. emitirá y publicará una Lista de Certificados Revocados (CRL) diariamente, y de forma extraordinaria, cada vez que se revoque un certificado.

LAZZATE CIA. LTDA. publicará cualquier modificación en la DPC y las Políticas de Certificación.

2.4. Control de acceso a los repositorios

La DPC, las Políticas de Certificación, las Condiciones Generales de Contratación, los certificados de CA y las listas de certificados revocados se publicarán en repositorios de

acceso público sin control de acceso.

Los certificados emitidos podrían ser publicados en repositorios públicos, siempre que el Suscriptor o el Firmante del certificado consienta de forma expresa esta acción. Los servicios de validación por el protocolo OCSP y TSP son de acceso público sin control de acceso y gratuitos.

3. Identificación y Autenticación

3.1. Registro de Nombres

3.1.1. Tipos de nombres

Todos los certificados requieren un nombre distinguido (DN o distinguished name) conforme al estándar X.500. Adicionalmente, los DN de los certificados cualificados son coherentes con lo dispuesto en las normas:

- ETSI EN 319 412 conocida como “European profiles for Qualified Certificates”
- 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”.

3.1.2. Necesidad de que los nombres sean significativos

Los atributos del DN del certificado referentes al nombre y apellidos de persona física se corresponderán con los datos del usuario / suscriptor, estos deberán estar detallados con exactitud a como están dispuesto en la cedula de identidad de ciudadanía, documento de residencia, pasaporte u otro medio reconocido en derecho dentro del Ecuador.

Los atributos del DN referentes a la denominación o razón social de persona jurídica, de entidad sin personalidad jurídica, o de autónomo o empresario individual se corresponderán con los datos del Suscriptor que consten en los registros oficiales del Servicio de Rentas Internas SRI y en los Registros Mercantiles del Ecuador. Los datos registrados deberán corresponder con exactitud a los expresados en el Registro Único de Contribuyentes (RUC) así como los contenidos en el Nombramiento de Representante Legal expedido por el Registro Mercantil.

En el caso que los datos consignados en el DN fueran ficticios o se indique expresamente su invalidez (ej. “PRUEBA” o “INVALIDO”), se considerará al certificado sin validez legal, únicamente válido para realizar pruebas técnicas de interoperabilidad (certificado de prueba), y que no cumple todo lo especificado en la presente DPC y en la PC correspondiente.

3.1.3. Uso de seudónimos

LAZZATE CIA. LTDA. no emite certificados con uso de seudónimos.

3.1.4. Reglas para interpretar varios formatos de nombres

LAZZATE CIA. LTDA. atiende en todo caso a lo marcado por el estándar X.500 de referencia en la ISO/IEC9594.

3.1.5. Unicidad de los nombres

El nombre distinguido (DN) de los certificados emitidos será único para cada Suscriptor y/o Firmante. Los atributos del DN que contienen el código identificativo del Suscriptor (NIF) y/o el código identificativo del Firmante (CIF) se usan para distinguir entre dos identidades cuando exista algún problema de duplicidad de nombres.

3.1.6. Reconocimiento, autenticación y papel de las marcas registradas

La CA no asume compromisos en la emisión de certificados respecto al uso por los Suscriptores de una marca comercial. LAZZATE CIA. LTDA. no permite deliberadamente el uso de un nombre cuyo derecho de uso no sea propiedad del Suscriptor. Sin embargo, la CA no está obligada a buscar evidencias de la posesión de marcas registradas antes de la emisión de los certificados.

3.2. Validación inicial de la identidad

3.2.1. Método de prueba de posesión de la clave privada

Cuando se emite un certificado en DCCF o DCCS portable o centralizado, o en otros dispositivos de los tipos dispositivo criptográfico portable o centralizado, o dispositivo software, la clave privada se crea en el instante previo a la generación del certificado, mediante un procedimiento que garantiza su confidencialidad y su vinculación con la identidad del Firmante o Creador de sello.

Cada RA y/o Tercer Vinculado es responsable de garantizar la entrega del dispositivo al Firmante o al Custodio de claves de forma segura.

En los otros casos, el método de prueba de la posesión de la clave privada por el Custodio de claves será la entrega de una petición PKCS #10 que contiene la correspondiente clave pública.

3.2.2. Autenticación de la identidad de una organización

3.2.2.1. Autenticación de la identidad de una persona jurídica

La Autoridad de Registro realizará la identificación y autenticación de la persona jurídica identificada en el certificado de sello electrónico (Suscriptor) o, en su caso, de la persona jurídica identificada en el certificado de firma electrónica (Suscriptor), conforme a los siguientes puntos:

1. La RA verificará los siguientes datos de la persona jurídica (Suscriptor):

- La denominación o razón social de la persona jurídica.
- Registro Único de Contribuyentes (RUC)
- Los datos relativos a la constitución y personalidad jurídica.
- Los datos relativos a la extensión y vigencia de las facultades de representación del Solicitante.

2. La RA podrá verificar los datos indicados en el punto 1 según uno de los siguientes procedimientos:

- Mediante los documentos, públicos si resultan exigibles, que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible.

- Mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

La RA se reserva el derecho de no aprobar la solicitud del certificado si considera que la documentación aportada no es suficiente o adecuada para la comprobación de los datos indicados en el punto 1.

3. El Solicitante deberá firmar la solicitud del certificado, declarando que sus datos de identidad y los datos de la persona jurídica incluidos en la misma son correctos.

La RA registrará los datos y documentos relativos a la identificación y autenticación de la persona jurídica identificada en el certificado de sello electrónico o, en su caso, de la persona jurídica identificada en el certificado firma electrónica.

3.2.3. Autenticación de la identidad de una persona natural

La Autoridad de Registro realizará la identificación y autenticación de la persona natural identificada en el certificado, conforme a los siguientes puntos:

1. Para la identificación de la persona natural se exigirá su personación y se acreditará mediante el Cédula de Identidad, el pasaporte u otros medios admitidos en Derecho. Podrá prescindirse de la personación de la persona física si el proceso de validación se realiza mediante validación biométrica o cualquier otro medio que garantice en derecho la identidad del suscriptor.

2. En el caso de un certificado de firma electrónica que contenga otros atributos de la persona física (Firmante), éstos deberán comprobarse mediante los documentos oficiales que los acrediten, como por ejemplo el Certificado del Registro Civil que acredite dicha información.

La RA se reserva el derecho de no aprobar la solicitud del certificado si considera que la documentación aportada no es suficiente o adecuada para la comprobación de los datos indicados.

3. La persona natural deberá firmar la solicitud del certificado, declarando que sus datos deidentidad y, en su caso, otros atributos personales incluidos en la misma son correctos.

La RA registrará los datos y documentos relativos a la identificación y autenticación del Solicitante y del Firmante del certificado de firma electrónica, o del Solicitante y del Custodio de claves del certificado de sello electrónico.

3.2.4. Validación del correo electrónico

Las direcciones de correo electrónico incluidas en los certificados y, en su caso, las de los Custodios de claves son validadas siempre por el Solicitante y, en su caso, también por el Firmante o por el Custodio de claves, mediante su inclusión en las respectivas solicitudes del certificado firmadas por el Solicitante, y por el Firmante o por el Custodio de claves y, en su caso, en la autorización firmada por el Solicitante.

3.3. Identificación y autenticación para solicitudes de renovación

3.3.1. Renovación de certificados en línea

Para los tipos de certificados que recojan en su Política de Certificación la renovación de certificados en línea, el Firmante se podrá identificar y autenticar en el proceso de renovación en línea utilizando su anterior certificado si éste cumple lo siguiente:

a) Está vigente (no ha caducado, ni ha sido revocado).
b) Quedan menos de 30 días para que caduque.
c) Para su emisión, se ha identificado al Suscriptor mediante la validación de la identidad ante la RA conforme a lo especificado en el apartado 3.2.3.

3.4. Identificación y autenticación para solicitudes de revocación

La identificación y autenticación del Suscriptor para una solicitud de revocación de un certificado podrá ser realizada por:

a) El propio Suscriptor, para los tipos de certificados que recojan en su Política de Certificación la revocación de certificados en línea, mediante el uso de la solicitud de revocación en línea una vez que el suscriptor se haya identificado con LAZZATE CIA. LTDA.

Requisitos operacionales en el ciclo de vida de los certificados

4.1. Solicitud de certificados

4.1.1. Quién puede solicitar un certificado

Los requisitos que debe reunir un Solicitante dependerán del tipo de certificado solicitado y estarán recogidos en la Política de Certificación de cada tipo de certificado concreto.

4.1.2. Proceso de solicitud de certificados

El Solicitante deberán ponerse en contacto con LAZZATE CIA. LTDA. por cualquiera de los canales habilitados para este proceso, ya sea web, presencial o por medio de unos de sus Terceros Vinculados, para gestionar la solicitud del certificado.

La ECIL proporcionará al Solicitante la siguiente información:

- Documentación necesaria para presentar para la tramitación de su solicitud y para verificarla identidad del Suscriptor y del Solicitante.
- Disponibilidad para realizar el proceso de registro.
- Información sobre el proceso de emisión y revocación, de la custodia de la clave privada, así como de las responsabilidades y las condiciones de uso del certificado y del dispositivo.
- Cómo poder acceder y consultar el presente documento, así como también las Políticas de Certificación y las Condiciones Generales de Contratación.

4.1.3. Rango de validez del certificado electrónico

En concordancia con lo expuesto en el Reglamento a la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos, en su decreto No. 3469, Art. 11, la duración de los certificados / firmas electrónicas es:

"*La duración del certificado defirma electrónica se establecerá contractualmente entre el titular de la firma electrónica y la entidad certificadora de información o quien haga sus veces. En caso de que las partes no acuerden nada al respecto, el certificado de firma electrónica se emitirá con una validez de dos años a partir de su expedición. Al tratarse de certificados de firma electrónica emitidos con relación al ejercicio de cargos públicos o privados, la duración del certificado de firma electrónica podrá ser superior a los dos años pero no podrá exceder el tiempo de duración de dicho cargo público o privado a menos que exista una de las prórrogas de funciones establecidas en las leyes.*"

4.2. Tramitación de las solicitudes de certificados

4.2.1. Realización de las funciones de identificación y autenticación

Es responsabilidad de la ECIL realizar de forma fehaciente la identificación y autenticación del Suscriptor. Este proceso deberá ser realizado previamente a la emisión del certificado, conforme a lo que se especificará en la Política de Certificación correspondiente a cada tipo de certificado.

4.2.2. Aprobación o denegación de las solicitudes de certificados

Una vez realizada la solicitud de certificado, el ECIL deberá verificar la información proporcionada por el Solicitante incluyendo la validación de la identidad del Solicitante.

Esta validación se realizará mediante la comparación de los datos y documentos suministrados por el solicitante.

La validación de la identidad del solicitante podrá ser:

- Física, en las instalaciones del ECIL
- Teleconferencia, con un operador del ECIL
- Biométrica, mediante la plataforma web del ECIL

Si la información no fuese correcta, el ECIL deberá denegar la petición, contactando con el Solicitante, y el Firmante o el Custodio de claves para comunicarles el motivo.

Si la información es correcta, y en el caso de la emisión de un Certificado de persona natural, se procederá a la firma del instrumento jurídico vinculante entre el Suscriptor y LAZZATE CIA. LTDA.. En el caso de la emisión de Certificados para Empresa y para la Función Pública, LAZZATE CIA. LTDA. verificará que el instrumento jurídico existe y que ha sido firmado, siendo responsabilidad del Solicitante verificar el cargo, título o rol declarado, así como, en su caso, su vinculación con la misma.

Se procederá entonces a la emisión del certificado.

4.3. Emisión de certificados

4.3.1. Acciones de la CA durante la emisión de los certificados

Una vez aprobada la solicitud se procederá a la emisión del certificado, que deberá ser entregado de forma segura al suscriptor.

- Para los certificados en soporte cualificado Hardware:

En el caso Token (dispositivo criptográfico portable), el ECIL le hará entrega al Suscriptor. En el caso de que el suscriptor un dispositivo criptográfico portable, se deberá verificar que este esté homologado por LAZZATE CIA. LTDA.

Activación del dispositivo: en el caso que el Suscriptor no disponga de ellos, se generarán los datos de activación del dispositivo y de acceso a la clave privada que contendrá el mismo.

Generación del par de claves: se procederá a la generación de las claves en el dispositivo utilizando el sistema proporcionado por la RA.

- Para los certificados en Otros dispositivos del tipo dispositivo software:

Se proporcionará un código de autenticación (OTP) al Suscriptor que deberá presentar para proceder con la generación del certificado, en la que se incluye la generación de las claves, la emisión del certificado y la descarga de ambos en formato PKCS #12 protegidos con una contraseña que él suscriptor debe establecer.

- En todos los casos:

La RA verificará el contenido de la petición de certificado, y si la verificación es correcta validará la petición.

La RA enviará a la CA por un canal seguro la clave pública en formato PKCS #10 junto con

el resto de los datos verificados que estarán contenidos en el certificado. Se procederá entonces a la generación del certificado en un procedimiento que utilizará protección contra falsificación y mantendrá la confidencialidad de los datos intercambiados.

Entrega del certificado: el certificado emitido será enviado a la RA, que lo pondrá a disposición del Suscriptor.

4.3.2. Notificación al Suscriptor de la emisión del certificado

La RA notificará al Suscriptor la emisión del certificado y el método de descarga si es necesario.

4.4. Aceptación del certificado

4.4.1. Forma en la que se acepta el certificado

El certificado se aceptará en el momento que el instrumento jurídico vinculante entre el Suscriptor y LAZZATE CIA. LTDA. haya sido firmado y el certificado haya sido entregado al Suscriptor, ya sea personal o telemáticamente.

Como evidencia de la aceptación, deberá quedar una hoja de aceptación firmada por el Suscriptor. El certificado se considerará válido a partir de la fecha en que se firmó la hoja de aceptación.

4.4.2. Publicación del certificado

Una vez que el certificado haya sido emitido y haya sido aceptado por el Suscriptor, el certificado podría ser publicado en los repositorios de certificados que se consideren necesarios.

4.5. Uso de las claves y el certificado

4.5.1. Uso de la clave privada y del certificado por el Suscriptor

Los certificados podrán ser utilizados según lo estipulado en esta DPC, en la Política de Certificación correspondiente. El par de claves emitido por el ECIL no están restringidas para su uso, de acuerdo con el estándar X509 V3 que por sus características son multi propósito: Firma Digital, Sin Repudio, Cifrado de Clave.

Las extensiones Key Usage y Extended Key Usage podrán ser utilizadas para establecer límites técnicos a los usos de la clave privada del certificado correspondiente. La aplicación de estos límites dependerá en gran parte de su correcta implementación por aplicaciones informáticas, quedando su regulación fuera del alcance de este documento.

La verificación de la validez del certificado en el momento del uso de la clave privada está determinada por el tipo de soporte en el que se emite el certificado y se indica en las políticas de cada tipo de certificado.

4.5.2. Uso de la clave pública y del certificado por los terceros que

confían en los certificados

Los terceros que confían en los certificados podrán utilizar los certificados para aquello que establece la presente DPC y la Política de Certificación correspondiente.

Es responsabilidad de los terceros verificar el estado del certificado mediante los servicios ofrecidos por LAZZATE CIA. LTDA. concretamente para ello y especificados en el presente documento.

4.6. Renovación de certificados sin cambio de claves

No se contempla esta opción.

4.7. Renovación con cambio de claves

LAZZATE CIA. LTDA. Autoridad de Certificación enviará una notificación de recordatorio de caducidad del certificado por correo electrónico al Suscriptor 30, 15 y 5 días antes de la fecha de caducidad del certificado.

Existen dos posibilidades para la renovación de certificados:

a) Proceso de renovación ante un Operador de RA, que se efectuará del mismo modo que la emisión de un certificado.

b) Proceso de renovación en línea, permitida sólo para los tipos de certificado que así estipulen en su Política de Certificación, que se detalla a continuación.

4.7.1. Circunstancias para la renovación en línea

Solamente se podrá proceder a la renovación en línea del certificado, según el tipo del certificado y si se cumplen las siguientes condiciones:

- Para su emisión, se ha identificado al Firmante mediante la validación de identidad ante un la RA conforme a lo especificado en el apartado 3.2.3.
- Está vigente (no ha caducado, ni ha sido revocado).
- Quedan menos de 30 días para que caduque.

4.7.2. ¿Quién puede pedir la renovación en línea de un certificado?

Cualquier Suscriptor de firma electrónica podrá pedir la renovación en línea de su certificado si se cumplen las circunstancias descritas en el punto anterior.

4.7.3. Tramitación de las peticiones de renovación en línea

Se realizarán los siguientes pasos:

- Se notificará al Suscriptor por correo electrónico que este habilitado para renovar su certificado.

- El Suscriptor deberá acceder a la página web de renovación de su certificado en www.enext.ec.
- Deberá autenticar su identidad según lo descrito y especificado en el apartado 3.2.3.
- Se procederá a la generación del nuevo par de claves.
- Se enviará por un canal seguro la clave pública a la CA en formato PKCS #10.
- Seguidamente se realizará la generación del certificado mediante un procedimiento que utilizará protección contra falsificación y mantendrá la confidencialidad de los datos intercambiados.
- El certificado generado será entregado al Suscriptor.

4.7.4. Notificación de la emisión del certificado renovado

La CA notificará al Firmante que el certificado ha sido renovado al finalizar correctamente el proceso.

4.7.5. Forma de aceptación del certificado renovado

El certificado se aceptará al firmar electrónicamente la renovación.

4.7.6. Publicación del certificado renovado

Una vez el certificado haya sido renovado, el nuevo certificado podría ser publicado en los repositorios de certificados que se consideren necesarios reemplazando al certificado anterior, siempre que el Suscriptor o el Firmante no se hubiera opuesto.

4.8. Modificación de certificados

En caso de necesidad de modificar algún dato, la RA deberá proceder a la revocación y a la emisión de un nuevo certificado.

4.9. Revocación de certificados

La revocación de un certificado supone la pérdida de validez de este y no podrá ser reversado. Las revocaciones tienen efecto desde el momento en que aparecen publicadas en la CRL.

4.9.1. Circunstancias para la revocación

Un certificado podrá ser revocado debido a las siguientes causas:

a) Circunstancias que afectan a la información contenida en el certificado:

- Comprobación de que los datos contenidos en la solicitud del certificado son falso o incorrecto.
- Modificación de cualquier dato contenido en el certificado.
- Extinción de la personalidad jurídica, o disolución de la entidad sin personalidad jurídica.

b) Circunstancias que afectan a la seguridad de la clave privada o del certificado:

- Compromiso o sospecha de compromiso de la clave privada o de la infraestructura o sistemas de la CA, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
- Infracción por parte de la CA o de la RA de los requisitos previstos en los procedimientos de gestión de certificados establecidos en la DPC o en la PC correspondiente.
- Compromiso o sospecha de compromiso de la seguridad de la clave privada o del certificado.
- Acceso o utilización no autorizados por un tercero de la clave privada del certificado.
- El incumplimiento por parte del Suscriptor de las normas de uso del certificado expuestas en la presente DPC, en la PC correspondiente o en el instrumento jurídico vinculante entre el ECIL y el Suscriptor.
- En caso de que se advierta que los mecanismos criptográficos utilizados para la generación de la clave privada o el certificado no cumplen los estándares de seguridad mínimos necesarios para garantizar su seguridad.

c) Circunstancias que afectan a la seguridad del dispositivo criptográfico:

- Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
- Pérdida o inutilización por daños del dispositivo criptográfico.
- Acceso no autorizado por un tercero a los datos de activación del dispositivo criptográfico.
- Incumplimiento por parte del Suscriptor de las normas de uso del dispositivo criptográfico expuestas en la presente DPC, en la PC correspondiente o en el instrumento jurídico vinculante entre el ECIL y el Suscriptor.

d) Circunstancias que afectan al Suscriptor:

- Finalización de la relación jurídica entre el ECIL y el Suscriptor.
- Modificación o extinción de la relación jurídica subyacente o causa que permitió la emisión del certificado al Firmante.
- Oposición o modificación, por parte del Suscriptor, de los datos contenidos en el fichero de datos de carácter personal de LAZZATE CIA. LTDA..
- Infracción por el Solicitante del certificado de los requisitos y obligaciones establecidos para la solicitud de este.
- Infracción por el Suscriptor, de sus obligaciones y responsabilidades establecidas en la presente DPC, en la PC correspondiente o en el instrumento jurídico correspondiente vinculante entre el ECIL y el Suscriptor.
- Capacidad modificada judicialmente o incapacidad sobrevenida, total o parcial,
- El fallecimiento del Firmante.
- Solicitud escrita por Suscriptor.

e) Otras circunstancias:

- Resolución judicial o administrativa que lo ordene.
- Cese de la actividad de una RA, salvo que expresamente se decida lo contrario (revocación masiva de todos de los certificados vigentes emitidos por esa RA).

- Por cualquier otra causa lícita especificada en la presente DPC o en la PC correspondiente.

4.9.2. Quién puede solicitar la revocación

Pueden solicitar la revocación de un certificado:

1. El Suscriptor, quien deberán solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.

2. LAZZATE CIA. LTDA., que deberán solicitar la revocación de un certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.

3. Cualquier otra persona podrá solicitar la revocación de un certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.

Podrán tramitar la solicitud de revocación del certificado:

- El Suscriptor, en los casos de revocación de certificados en línea.

- Los operadores autorizados de LAZZATE CIA. LTDA. (Responsables de Revocación).

En todo caso, al tiempo de revocarse el certificado, se enviará un comunicado por correo electrónico al Suscriptor, especificando la fecha y la hora y el motivo de la revocación.

4.9.3. Procedimientos de solicitud de revocación

Existen distintas alternativas para solicitar la revocación de un certificado.

El suscriptor, recibirá una comunicación del sistema informándole que se ha producido la revocación del certificado, indicando la fecha, la hora y la causa de la revocación.

4.9.3.1. Procedimiento en línea

Para los tipos de certificados que recojan en su Política de Certificación la revocación de certificados en línea, LAZZATE CIA. LTDA. pondrá a disposición del Suscriptor, un formulario web desde el que podrá realizar y tramitar la solicitud de revocación de su certificado.

Este mecanismo de solicitud de revocación se convierte en el principal para todos los certificados emitidos por cualquier Operador de RA, de tal forma que se garantiza que cualquier certificado puede ser revocado en menos de 24 horas.

El proceso de revocatoria por parte del propio suscriptor es online:

- El Suscriptor deberá ingresar en la plataforma de la ECIL con los datos con los que se registró para emitir su certificado de firma electrónica.
- Deberá escoger la opción revocatoria de certificado del menú de opciones y firmará la solicitud de revocatoria con una firma certificada que se le emitirá en ese momento. Dicha firma no tendrá costo adicional.

- Se procederá de informa inmediata a revocar el certificado del Suscriptor.

Todas las revocaciones son efectivas desde el momento en que son publicadas en la CRL de la ECIL.

Este proceso asume la aceptación explícita de la tramitación de la solicitud de revocación y las consecuencias de ésta.

Una vez aceptada la tramitación, el certificado será inmediatamente revocado.

La RA recibirá una comunicación del sistema informándole que se ha producido la revocación del certificado.

4.9.3.2. Procedimientos internos

LAZZATE CIA. LTDA., y las Autoridades de Registro podrán solicitar la revocación de certificados mediante procedimientos internos.

Un operador autorizado de LAZZATE CIA. LTDA. (Responsable de Revocación) deberá identificar y autenticar al solicitante de la revocación mediante los procedimientos que considere oportunos, y comprobar que la causa comunicada se corresponde con alguna de las circunstancias anteriormente indicadas.

Una vez correctamente identificado el solicitante de la revocación y comprobada la causa comunicada, el operador procederá a tramitar la solicitud de revocación.

4.9.3.3. Revocación telefónica

LAZZATE CIA. LTDA. dispone de un servicio de revocación telefónico en el que se podrá solicitar la revocación de un certificado, en horarios de oficina:

Servicio de revocación telefónico (horario de oficina[3]): +593 500 01500

Un operador autorizado de LAZZATE CIA. LTDA. (Responsable de Revocación) deberá identificar y autenticar al solicitante de la revocación mediante los procedimientos que considere oportunos, y comprobar que la causa comunicada se corresponde con alguna de las circunstancias anteriormente indicadas.

Además, en el caso de que la revocación del certificado sea solicitada por una persona distinta al Suscriptor, el operador deberá verificar la causa de revocación comunicada mediante los procedimientos que considere oportunos.

Una vez correctamente identificado el solicitante de la revocación y comprobada y, en su caso, verificada la causa comunicada, el operador procederá a tramitar la solicitud de revocación.

4.9.4. Plazo en el que la CA debe procesar la solicitud de revocación

El tiempo máximo desde la recepción de la solicitud de revocación hasta su confirmación y

tramitación será de 24 horas. Si en ese tiempo no se puede confirmar la solicitud de revocación, ésta no será tramitada.

Una vez que la solicitud de revocación haya sido confirmada y debidamente tramitada, será procesada por la CA inmediatamente.

4.9.10. Obligación de verificación de las revocaciones por los terceros que confían en los certificados

La verificación del estado de los certificados es obligatoria para cada uso de los certificados, ya sea mediante la consulta de la CRL o del servicio OCSP.

4.9.11. Frecuencia de emisión de las CRL

La CRL de los certificados de entidad final se emite cada 24 horas. La ECIL emitirá también una CRL cada 2 horas.

Una vez emitida la CRL de los certificados de CA (ARL), ésta se publica cada 4 meses.

4.9.12. Tiempo máximo entre la generación y la publicación de las CRL

Una vez emitida la CRL de los certificados de CA (ARL), ésta se publicada y actualiza de forma automática.

4.9.13. Disponibilidad de sistemas en línea de verificación del estado de los certificados

LAZZATE CIA. LTDA. tiene disponible el sistema en línea de verificación del estado de los certificados,el cual está disponible las 24 horas del día, 7 días de la semana.

4.9.14. Requisitos de comprobación de revocación en línea

Para el uso del sistema de comprobación de revocación en línea por CRL, de libre acceso, deberá considerarse lo siguiente:

- Se deberá comprobar el estado de revocación del certificado de entidad final en la última CRL emitida y publicada por la CA Subordinada de LAZZATE CIA. LTDA., que podrá descargarse en la dirección URL contenida en el propio certificado, en su extensión CRL DistributionPoints.

- Se deberá comprobar que cada CRL esté vigente (con un valor del campo *nextUpdate* posterior a la fecha y hora actuales) y firmada por la CA que ha emitido el certificado que se quiere validar.

- Los certificados revocados que expiren son retirados de las CRL, excepto en el caso de

4.10. Servicios de información del estado de los certificados

5.1.1. Características operativas

LAZZATE CIA. LTDA. ofrece un servicio gratuito de publicación en Web de Listas de Certificados Revocados (CRL), sin restricciones de acceso, en las direcciones indicadas en el apartado 2.1, así como en los certificados, en su extensión CRL Distribution Points.

LAZZATE CIA. LTDA. ofrece un servicio gratuito de validación de certificados por medio del protocolo OCSP, sin restricciones de acceso, en la dirección indicada en el apartado 2.1, así como en los certificados, en su extensión Authority Information Access.

Adicionalmente, LAZZATE CIA. LTDA. puede ofrecer otros servicios comerciales de validación de certificados.

5.1.2. Disponibilidad del servicio

La información relativa al estado de los certificados estará disponible en línea las 24 horas del día, los 7 días de la semana.

En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de LAZZATE CIA. LTDA., éste realizará los mayores esfuerzos para asegurar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo de 24 horas.

En el caso del cese de actividad de la CA de LAZZATE CIA. LTDA. sin trasferencia de la gestión de los certificados emitidos a otro Ente de Certificación, se realizará una revocación masiva de todos los certificados vigentes emitidos y se emitirá y publicará una última CRL que tendrá un valor del campo *nextUpdate* igual a la fecha y hora UTC 31/12/9999 23:59:59 y contendrá todos los certificados revocados, incluyendo aquéllos que hubiesen expirado y la extensión X.509 ExpiredCertsOnCRL. Esta última CRL de la CA de LAZZATE CIA. LTDA. estará disponible durante al menos 15 años desde su emisión, mientras que el servicio OCSP de la CA de LAZZATE CIA. LTDA. dejará de estar disponible.

La provisión de la información sobre el estado de los certificados queda garantizada en el caso de cese de la actividad de LAZZATE CIA. LTDA. como CA, mediante la transferencia de la gestión de los certificados emitidos a otro Ente de Certificación, quien conservará la información relativa a los servicios de certificación prestados hasta entonces por LAZZATE CIA. LTDA., o mediante la comunicación a la administración competente de la información relativa a todos los certificados cualificados expedidos cuya vigencia habrá sido extinguida, para que se haga cargo de su custodia.

5.2. Finalización de la suscripción

La suscripción del certificado finalizará en el momento de expiración o revocación del certificado.

6. Controles de seguridad física, instalaciones, gestión y operaciones

Lazzate garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información, del cual hace parte integral la presente política, por medio de la creación de una comisión técnica denominada Comité de Seguridad de la Información.

La información es un recurso que, como el resto de los activos, tiene valor para Lazzate y por consiguiente debe ser debidamente protegida.

El establecimiento, seguimiento, mejora continua y aplicación de la Política de Seguridad de la Información garantiza un compromiso ineludible de protección a la misma frente a una amplia gama de amenazas. Con esta política se contribuye a minimizar los riesgos asociados de daño y se asegura el eficiente cumplimiento de las funciones sustantivas de la entidad apoyadas en un correcto sistema de información.

Lazzate establecerá los mecanismos para respaldar la difusión, estudio, actualización y consolidación tanto de la presente política como de los demás componentes del Sistema de Gestión de la Seguridad de la Información y alinearlos de forma efectiva con los demás sistemas de gestión.

6.1. Controles físicos

LAZZATE CIA. LTDA. tienen establecidos controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas y los equipamientos empleados para las operaciones.

La política de seguridad física y ambiental aplicable a los servicios de la ECIL ofrece protección frente:

- Controles de acceso y seguridad física.
- Desastres naturales.
- Detección de incendio y sistemas de extinción de conflagraciones
- Controles de humedad y temperatura.
- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).
- Derrumbamiento de la estructura.
- Bajo riesgo de inundación.
- Robo.

Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios la ECIL.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año, con asistencia en las 24 horas siguientes al aviso. La localización de las instalaciones garantiza la presencia de fuerzas de seguridad en un plazo no superior a 30 minutos.

6.1.1. Ubicación física y construcción

Las instalaciones están construidas con materiales que garantizan la protección frente a ataques por fuerza bruta, están ubicadas en una zona de bajo riesgo de desastres y permiten

un rápido acceso.

La sala donde se realizan las operaciones criptográficas de las CA y RA D tiene un diseño estructural Antincendios, Sistema de Detección Inteligente de incendio/ Elemento de Extinción, resistente a inundaciones, vendavales y descargas eléctricas, sistemas anti-humedad, doble sistema de refrigeración y plantas de generación eléctrica.

6.1.2. Acceso físico

El acceso físico a las dependencias donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales.

El acceso está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro de este, incluyendo filmación por sistema de seguridad con cámaras de video. Todas las instalaciones de la ECIL cuentan con detectores de movimiento y apertura en todos los puntos vulnerables, así como sistemas de alarma para detección de intrusión con aviso por canales alternativos.

El acceso a las salas de las plataformas de las CA y las RA se realiza con lectores huella dactilar y cifrado numérico, gestionado por un sistema informático que mantiene un log de entradas y salidas automático.

6.1.3. Alimentación eléctrica y aire acondicionado

Las instalaciones disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado mediante un grupo electrógeno redundante con depósitos de combustible que pueden ser rellenados desde el exterior.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado duplicado.

6.1.4. Exposición al agua

Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

6.1.5. Protección y prevención de incendios

Las salas donde se albergan equipos informáticos disponen de sistemas de detección y extinción de incendios automáticos.

6.1.6. Sistema de almacenamiento

En las instalaciones de las plataformas de las CA, cada medio de almacenamiento desmontable (cintas, cartuchos, disquetes, etc.), que contenga información clasificada, está etiquetado con el nivel más alto de clasificación de la información que contenga y permanece solamente al alcance de personal autorizado. La información con clasificación *Confidencial*, independientemente del dispositivo de almacenamiento, se guarda en armarios ignífugos o bajo llave permanentemente, requiriéndose autorización expresa para su retirada.

En las instalaciones de las plataformas de las RA gestionadas por LAZZATE CIA. LTDA., los

sistemas de los servidores se ejecutan mediante el despliegue de un entorno virtualizado en alta disponibilidad, soportado sobre dispositivos redundantes de computación, almacenamiento de alto rendimiento y redes independientes de producción, gestión y almacenamiento.

6.1.7. Eliminación de los soportes de información

Cuando haya dejado de ser útil, la información sensible es destruida en la forma más adecuada al soporte que la contenga:

- Impresos y papel: mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.
- Medios de almacenamiento: antes de ser desechados o reutilizados, deben ser procesados para su borrado, mediante su destrucción física o haciendo ilegible la información contenida.

6.1.8. Copias de seguridad fuera de las instalaciones

LAZZATE CIA. LTDA. mantienen un almacén externo seguro para la custodia de documentos en papel, y de dispositivos y documentos electrónicos independiente del centro de datos.

Se requieren de dos personas autorizadas para el acceso, depósito o retirada de dispositivos, documentos, etc.

6.2. Controles de procedimiento

6.2.1. Roles de confianza

Los roles de confianza garantizan una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de certificación.

- Responsable de Seguridad (*Security Officers*): mantiene la responsabilidad global sobre la administración y la implementación de las políticas y procedimientos de seguridad.
- Operadores de RA (*Registration Officers*): responsables de verificar la información necesaria para emitir los certificados y de aprobar las solicitudes de certificados.
- Responsables de Revocación (*Revocation Officers*): responsables de realizar los cambios en el estado de un certificado.
- Administradores del Sistema de Certificación (*System Administrators*): autorizados para instalar, configurar y mantener los sistemas para la administración de los servicios.
- Operadores de Sistemas (*System Operators*): responsables de operar día a día los sistemas. Autorizados para realizar backup de los sistemas.
- Auditores Internos (*System Auditors*): autorizados para ver los *logs* de los sistemas.

Adicionalmente, se establecen los siguientes roles de confianza específicos de las plataformas de las CA y las RA:

- Operadores de CA - Operadores de Certificación: responsables de activar las claves de la CA de LAZZATE CIA. LTDA. en su entorno en línea, y de los procesos de firma de certificados y CRL en el entorno offline de la CA Raíz.
- Administradores de Operadores RA: responsables de realizar las funciones de dar de alta a los operadores en las plataformas de las RA.

6.2.2. Número de personas requeridas por tarea

La CA garantiza al menos dos personas para realizar las tareas que requieren control *multipersona* y que se detallan a continuación:

- La generación de las claves de las CA.
- La recuperación de un back-up de la clave privada de las CA.
- La emisión de certificados de las CA.
- Activación de la clave privada de las CA.
- Cualquier actividad realizada sobre los recursos hardware y software que dan soporte a la CA Raíz.

6.2.3. Identificación y autenticación por rol

Cada persona sólo 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, tarjetas de acceso físico y llaves.

6.2.4. Roles que requieren segregación de funciones

Se establecen las siguientes incompatibilidades entre los roles establecidos en el apartado 5.2.1, de forma que una persona no pueda tener dos roles incompatibles:

- El rol Responsable de Seguridad (*Security Officer*) es incompatible con cualquier otro rol.
- Los roles de Operadores de RA (*Registration Officers*) y Responsables de Revocación (*Revocation Officers*) son incompatibles con los roles de Administradores del Sistema de Certificación (*System Administrators*), Operadores de Sistemas (*System Operators*) yOperadores de CA - Operadores de Certificación.

6.3. Controles de personal

6.3.1. Requisitos relativos a la calificación, conocimiento y experiencia profesionales

Todo el personal que realiza tareas calificadas como confiables sin supervisión lleva al menos dos meses trabajando en LAZZATE CIA. LTDA., y mantiene un contrato de trabajo fijo.

Todo el personal está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

Tanto los ejecutivos de LAZZATE CIA. LTDA. como el personal con roles de confianza están libres de cualquier presión comercial, financiera u de otra índole que pudiere influir negativamenteen la confianza en los servicios que presta.

LAZZATE CIA. LTDA. se asegura que los operadores de registro (RA) son personal confiable de LAZZATE CIA. LTDA. o de la Entidad que asume funciones de RA.

El operador de registro habrá realizado un curso de preparación para la realización de las tareas de registro y validación de las solicitudes de certificados. Al final de dicho curso, LAZZATE CIA. LTDA. o un tercero designado por LAZZATE CIA. LTDA. procederá a evaluar sus conocimientos de los procedimientos relativos a la emisión de certificados por la CA de LAZZATE CIA. LTDA., para asegurar la correcta realización de las tareas asignadas a su rol.

LAZZATE CIA. LTDA. retirarán de sus funciones de confianza a cualquier empleado y/o funcionario de la ECIL cuando tengan conocimiento de la existencia de algún hecho delictivo que pudiera afectar al desempeño de estas funciones.

6.3.2. Procedimientos de comprobación de antecedentes

LAZZATE CIA. LTDA. realizan las investigaciones pertinentes antes de la contratación de cualquier persona para realizar funciones de confianza.

6.3.3. Requerimientos de formación

LAZZATE CIA. LTDA. 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.

6.3.4. Requerimientos y frecuencia de actualización de laformación

Se realizarán actualizaciones de formación al personal al menos cuando se realicen modificaciones en las tareas asignadas a un rol que así lo requieran, o cuando lo solicite alguna persona.

6.3.5. Sanciones por actuaciones no autorizadas

LAZZATE CIA. LTDA. disponen de un régimen sancionador interno por la realización de acciones no autorizadas pudiéndose llegar al cese del trabajador.

6.3.6. Requisitos de contratación de terceros

Los empleados contratados para realizar tareas confiables deberán firmar con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados por el PSC. Cualquier acción que comprometa la seguridad de los procesos críticos aceptados podrá dar lugar al cese del contrato laboral.

6.4. Procedimientos de auditoría de seguridad

6.4.1. Tipos de eventos registrados

LAZZATE CIA. LTDA. registran y guardan los *logs* de todos los eventos relativos al sistema de seguridad de las CA y las RA. Estos incluyen los siguientes eventos:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la CA o las RA a través de la red.
- Intentos de accesos no autorizados a la red interna de la CA.
- Intentos de accesos no autorizados al sistema de archivos.
- Intentos de creación, borrado y establecimiento de contraseñas en el hardware criptográfico.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de las CA y las RA.
- Encendido y apagado de las aplicaciones de las CA y las RA.
- Cambios en los detalles de las CA y/o sus claves.
- Cambios en la creación de perfiles de certificados.
- Generación de claves propias.
- Eventos del ciclo de vida de los certificados.
- Eventos asociados al uso del módulo criptográfico de la CA.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.

Adicionalmente, LAZZATE CIA. LTDA. y las RA registran:

- Los cambios en la política de seguridad
- Los colapsos del sistema
- Los fallos en el hardware
- Las actividades de los cortafuegos y enrutadores.
- La documentación presentada por el solicitante, así como toda la información del proceso de registro.
- Todos los sucesos relacionados con la preparación de los dispositivos DCCF

LAZZATE CIA. LTDA. conservan, ya sea física o electrónicamente, la siguiente información:

- Las ceremonias de creación de claves de las CA y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimiento y cambios de configuración del sistema.
- Cambios en el personal que realiza tareas de confianza en las CA y las RA.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del Solicitante, y del Firmante o del Custodio de

Claves, si se gestiona esa información.

- Posesión de datos de activación, para operaciones con la clave privada de las CA.

6.4.2. Frecuencia de procesado de registros de auditoría

Se revisarán los logs de auditoría en un plazo de tiempo que se determinará por el comité de seguridad de LA ECIL, y en todo caso cuando se produzca una alerta del sistema motivada por la existencia de algún incidente, en busca de actividad sospechosa o no habitual.

6.4.3. Periodo de conservación de los registros de auditoría

Se almacenará la información de los logs de auditoría durante al menos 15 años (en el caso de eventos del ciclo de vida de los certificados, desde el momento de la expiración del certificado) para garantizar la seguridad del sistema.

6.4.4. Protección de los registros de auditoría

Los logs de los sistemas son protegidos de su manipulación mediante mecanismos que aseguran su integridad. Los logs son almacenados en dispositivos ignífugos.

En el caso de las plataformas de las CA, se protege la disponibilidad de los logs mediante el almacén en instalaciones externas al centro de datos.

Los dispositivos son manejados en todo momento por personal autorizado.

6.4.5. Procedimientos de respaldo de los registros de auditoría

LAZZATE CIA. LTDA. disponen de un procedimiento adecuado de backup, de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

En la CA, se tiene implementado un procedimiento de backup seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo. El medio externo se almacena en armario ignífugo bajo medidas de seguridad que garantizan que su acceso solo está permitido a personal autorizado.

Adicionalmente, se mantiene copia de los logs de auditoría en un centro de custodia externo.

6.4.6. Sistema de recogida de información de auditoría

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo y por el software de certificación.

6.4.7. Análisis de vulnerabilidades

En el caso de las plataformas de las CA, se realiza periódicamente una revisión de discrepancias en la información de los *logs* y actividades sospechosas, así como análisis de vulnerabilidades de direcciones IP internas y externas, de acuerdo con el procedimiento

interno establecido al efecto en las políticas de seguridad.

En el caso de las plataformas de la RA de LAZZATE CIA. LTDA., se realiza periódicamente una revisión de vulnerabilidades y test de intrusión. Después, se analizarán y se corregirán las vulnerabilidades que se crea que son un riesgo.

6.5. Archivo de registros

6.5.1. Tipos de registros archivados

Se conservarán los datos del sistema que tengan lugar durante el ciclo de vida del certificado, incluyendo su renovación. Se almacenarán por LAZZATE CIA. LTDA. o, por delegación de ésta, por un Tercer Vinculado:

- Todos los registros de auditoría (*logs*).
- Todos los datos relativos a los certificados, incluyendo los contratos con los Suscriptores, y cualquier información relativa a la identificación y autenticación de los Suscriptores, y a la solicitud, aceptación y entrega de los certificados.
- Solicitudes de emisión y revocación de certificados.
- Todos los certificados emitidos.
- CRL emitidas o registros del estado de los certificados generados (consultas OCSP).

6.5.2. Periodo de conservación de registros

Todos los datos del sistema relativos al ciclo de vida de los certificados se conservarán durante al menos 15 años desde el momento de la expiración del certificado. En particular:

- Los certificados se conservarán durante al menos 15 años desde su expiración.

- Los contratos con los Suscriptores, y cualquier información relativa a la identificación y autenticación de los Suscriptores, de los Solicitantes, y de los Firmantes o de los Custodios de claves, y a la solicitud, aceptación y entrega de los certificados serán conservados durante al menos 15 años desde el momento de la expiración del certificado.

- En el caso del cese de actividad de la CA de LAZZATE CIA. LTDA. sin trasferencia de la gestión de los certificados emitidos a otro PSC, se conservará la última CRL emitida por la CA de LAZZATE CIA. LTDA., después de realizar una revocación masiva de todos los certificados vigentes emitidos, durante al menos 15 años desde su emisión.

6.5.3. Protección del archivo

LAZZATE CIA. LTDA. aseguran la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas y/o instalaciones externas, en los casos en que así se requiera.

Además, se dispone de documentos técnicos y de configuración donde se detallan todas las acciones tomadas para garantizar la protección de los archivos.

6.5.4. Procedimientos de copia de seguridad del archivo

LAZZATE CIA. LTDA. disponen de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido solo a personal autorizado.

6.5.5. Requerimientos para el sellado de tiempo de los registros

Los registros están fechados con una fuente fiable.

Existe dentro de la documentación técnica y de configuración de la CA un apartado sobre la configuración de tiempos de los equipos utilizados en la emisión de certificados.

6.5.6. Procedimientos para obtener y verificar información archivada

Los eventos registrados están protegidos contra manipulaciones no autorizadas, los mismos que pueden ser verificados por una auditoria.

Sólo el personal autorizado para ello tiene acceso a los archivos físicos de soportes y archivos informáticos, para obtener y llevar a cabo verificaciones de integridad de dichos archivos.

6.6. Cambio de claves y/o certificado de las CA

6.6.1. CA Raíz

En el momento en el que el ECIL lo considere conveniente y, en todo caso, antes de que expiren todos los certificados que contienen la clave pública de la CA Raíz, se generará un nuevo certificado de la CA Raíz, pudiendo optar por una de las siguientes posibilidades:

1. Sustitución del certificado de la CA Raíz sin cambio de claves.

La CA Raíz seguirá usando la misma clave privada y tendrá el nuevo certificado, que contendrá la misma clave pública y el mismo DN en el campo subject que su anterior certificado.

El nuevo certificado de la CA Raíz se publicará en los repositorios de LAZZATE CIA. LTDA. en las mismas URL que su anterior certificado.

Las nuevas CRL de la CA Raíz (ARL) se publicarán en los repositorios de LAZZATE CIA. LTDA. en las mismas URL que las anteriores CRL.

2. Sustitución del certificado de la CA Raíz con cambio de claves (*rekeying*). En este caso, se generará una nueva CA Raíz.

La nueva CA Raíz usará la nueva clave privada y tendrá el nuevo certificado auto firmado, que contendrá la nueva clave pública y un DN en el campo subject distinto al contenido en su anterior certificado de la CA Raíz.

La clave privada de la anterior CA Raíz sólo se usará para la firma de sus CRL (ARL) mientras existan certificados vigentes emitidos por la anterior CA Raíz y, después, para la firma de una última CRL.

Cuando se deje de usar la clave privada de la anterior CA Raíz, ésta será destruida.

El certificado de la nueva CA Raíz se publicará en los repositorios de LAZZATE CIA. LTDA. y El ECI LAZZATE CIA. LTDA. en URL distintas a las de la anterior CA Raíz.

Las CRL de la nueva CA Raíz (ARL) se publicarán en los repositorios de LAZZATE CIA. LTDA. y El ECI LAZZATE CIA. LTDA. en URL distintas a las de la anterior CA Raíz.

En todos los casos de sustitución del certificado de la CA Raíz, se podrán introducir cambios en su contenido, para que se ajuste mejor a la normativa y la legislación vigentes y/o a la realidad de El ECI LAZZATE CIA. LTDA. y del mercado.

6.6.2. CA Subordinada de LAZZATE CIA. LTDA.

En el momento en el que LAZZATE CIA. LTDA. lo consideren conveniente y, en todo caso, antes de que expiren o sean revocados todos los certificados emitidos por la CA Raíz que contienen la clave pública de la CA Subordinada de LAZZATE CIA. LTDA., se emitirá un nuevo certificado de la CA Subordinada de LAZZATE CIA. LTDA. firmado por la CA Raíz, pudiendo optar por una de las siguientes posibilidades:

1. Sustitución del certificado de la CA Subordinada de LAZZATE CIA. LTDA. sin cambio de claves.

La CA Subordinada de LAZZATE CIA. LTDA. seguirá usando la misma clave privada y tendrá el nuevo certificado firmado por la CA Raíz, que contendrá la misma clave pública y el mismo DN en el campo subject que su anterior certificado.

El nuevo certificado de la CA Subordinada de LAZZATE CIA. LTDA. se publicará en los repositorios de LAZZATE CIA. LTDA. en las mismas URL que su anterior certificado.

Las nuevas CRL de la CA Subordinada de LAZZATE CIA. LTDA. se publicarán en los repositorios de LAZZATE CIA. LTDA. en las mismas URL que las anteriores CRL.

2. Sustitución del certificado de la CA Subordinada de LAZZATE CIA. LTDA. con cambio de claves .

En este caso, se podrá optar por una de las siguientes posibilidades:

a) Generar una nueva CA Subordinada de LAZZATE CIA. LTDA.

La nueva CA Subordinada de LAZZATE CIA. LTDA. usará la nueva clave privada y tendrá el nuevo certificado firmado por la CA Raíz, que contendrá la nueva clave pública y un DN en el campo subject distinto al contenido en su anterior certificado.

La clave privada de la anterior CA Subordinada de LAZZATE CIA. LTDA. sólo se usará para

la firma de sus CRL mientras existan certificados vigentes emitidos por dicha CA y, después, para la firma de una última CRL.

Cuando se deje de usar la anterior clave privada de la CA Subordinada de LAZZATE CIA. LTDA., ésta será destruida.

El certificado de la nueva CA Subordinada de LAZZATE CIA. LTDA. se publicará en los repositorios de LAZZATE CIA. LTDA. en URL distintas a las de la anterior CA Subordinada de LAZZATE CIA. LTDA..

Las CRL de la nueva CA Subordinada de LAZZATE CIA. LTDA. se publicarán en los repositorios de LAZZATE CIA. LTDA. en URL distintas a las de la anterior CA Subordinada de LAZZATE CIA. LTDA..

b) No generar una nueva CA Subordinada de LAZZATE CIA. LTDA..

La CA Subordinada de LAZZATE CIA. LTDA. usará la nueva clave privada y tendrá el nuevo certificado firmado por la CA Raíz, que contendrá la nueva clave pública y el mismo DN en el campo subject que su anterior certificado.

La anterior clave privada de la CA Subordinada de LAZZATE CIA. LTDA. no se volverá a usar desde el momento en que se empiece a usar la nueva clave privada.

Cuando se deje de usar la anterior clave privada de la CA Subordinada de LAZZATE CIA. LTDA., ésta será destruida.

El nuevo certificado de la nueva CA Subordinada de LAZZATE CIA. LTDA. se publicará en los repositorios de LAZZATE CIA. LTDA. en URL distintas a las de su anterior certificado.

Las nuevas CRL de la CA Subordinada de LAZZATE CIA. LTDA. se publicarán en los repositorios de LAZZATE CIA. LTDA. en las mismas URL que las anteriores CRL.

En todos los casos de sustitución del certificado de la CA Subordinada de LAZZATE CIA. LTDA., se podrán introducir cambios en su contenido, para que se ajuste mejor a la normativa y la legislación vigentes y/o a la realidad de LAZZATE CIA. LTDA. y del mercado.

6.7. Plan de recuperación de desastres

6.7.1. Procedimientos de gestión de incidentes y vulnerabilidades

La política de seguridad de LAZZATE CIA. LTDA., determina que la CA recuperará la funcionalidad de sus sistemas en un plazo máximo de 48 horas.

Los servicios de revocación y presentación de listados de certificados revocados estarán disponibles en 24 horas.

6.7.2. Alteración de los recursos hardware, software y/o datos

En el caso de que tuviera lugar un incidente que alterara o corrompiera recursos hardware, software, así como datos, LAZZATE CIA. LTDA. procederán de acuerdo con la Política de Seguridad de la ECIL.

6.7.3. Procedimiento de actuación ante la vulnerabilidad de la clave privada de la Autoridad de Certificación

En el evento de que existiera o se encuentre comprometida la clave privada de la CA de LAZZATE CIA. LTDA.:

- Como mínimo, mediante la publicación de un aviso en el portal web de LAZZATE CIA. LTDA., notificará del compromiso de la clave privada de la CA a todos los Suscriptores, o entidades con los cuales tenga acuerdos u otro tipo de relación.

- Indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave privada no son válidos.

- La CA cuenta con un centro de contingencia adicional para poner en funcionamiento todos los sistemas de certificación.

- En función a lo que estipula la DPC de la ECIL, los servicios de revocación y publicación de certificados revocados dentro de 24 horas posterior a cualquier desastre o emergencia.

6.7.4. Continuidad del negocio después de un desastre

LAZZATE CIA. LTDA. En función a lo que estipula la DPC de la ECIL, los servicios de revocación y publicación de certificados revocados dentro de 24 horas posterior a cualquier desastre o emergencia.

La CA cuenta con un centro de contingencia adicional para poner en funcionamiento todos los sistemas de certificación.

6.8. Cese de actividad

6.8.1. Autoridad de Certificación (CA)

Antes del cese de su actividad como CA, LAZZATE CIA. LTDA. realizará las siguientes actuaciones:

- Proveerá de los fondos necesarios para continuar la finalización de las actividades de revocación hasta el cese definitivo de la actividad, si es el caso.
- Notificar al organismo de control (ARCOTEL), con por lo menos 90 días de anticipación, sobre el cese de actividades.
- Notificar a sus usuarios, suscriptores y Terceros Vinculados, con por lo menos 90 días de anticipación, sobre el cese de actividades.
- Realizar por lo menos una publicación dirigida a sus usuarios y Terceros Vinculados, informando del cese de actividades, en nuestro portal web y diferentes redes sociales

que maneje Lazzate.

- Dar por terminados todos los contratos de Tercera Vinculación con entidades que utilicen nuestra CA.
- La CA dejará de emitir certificados.
- Eliminar todas las claves privadas de la CA.
- Revocar todos los certificados que se hubieren emitido con nuestra CA.
- Todos los registros y archivos digitales de la CA serán transferidos a un custodio seleccionado por la CA.

6.8.2. Autoridad de Registro (AR)

Ante el cese de actividad de una Autoridad de Registro de LAZZATE CIA. LTDA.:

- Deberá notificar con 60 días de anticipación su voluntad de cese de actividades.
- Una vez recibida la notificación deberá dejar de emitir y renovar certificados.
- Deberá revocar los certificados emitidos a favor de dicho Tercer Vinculado.
- Prestará toda su voluntad y colaboración para que el equipo técnico y auditor de Lazzate pueda verificar que el cese se llevó a cabo bajo los lineamientos específicos requeridos por Lazzate.

A su vez, la RA:

- Entregará toda la documentación asociada a la emisión y gestión de los certificados, yasea en formato papel o electrónico, a LAZZATE CIA. LTDA.

6. Controles de seguridad técnica

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

La generación de las claves de la CA Raíz y la CA Subordinada de LAZZATE CIA. LTDA. se realiza, de acuerdo con un procedimiento documentado de ceremonia de claves, dentro de una sala de seguridad, en un dispositivo criptográfico hardware (HSM), por personal autorizado según los roles de confianza con un control dual, y en presencia de testigos y un auditor externo.

LAZZATE CIA. LTDA. garantizan que las claves de firma de la CA Raíz y la CA Subordinada de LAZZATE CIA. LTDA. no son empleadas para otro supuesto quelos indicados en este documento.

Para los certificados de los Suscriptores:

- En dispositivo hardware portable o centralizado, en otros dispositivos de los tipos dispositivo criptográfico portable o centralizado:

El par de claves será generado en el mismo dispositivo utilizando el sistema proporcionado por la RA.

Este proceso está vinculado de forma segura al proceso de generación del certificado, garantizando la confidencialidad de la clave privada durante el proceso de generación y la complementariedad entre los datos de creación de firma o sello electrónicos (clave privada) y los datos de validación (clave pública).

- En dispositivo software:

El Suscriptor claves recibirá por correo electrónica la confirmación de la solicitud, juntamente con un código de autenticación a la aplicación en línea de generación de certificados.

Para poder acceder a la aplicación en línea de generación de certificados, será necesario que el Suscriptor proporcione el código de autenticación recibido.

Una vez autenticado, el Suscriptor procederá a la generación del certificado (incluye la generación del par de claves, la emisión del certificado y la descarga de ambos en formato PKCS #12 protegido con una contraseña que él mismo habrá establecido).

- En Otros dispositivos del tipo dispositivo externo:

El par de claves habrá sido generado previamente en un dispositivo externo gestionado por el Suscriptor y/o el Custodio de claves.

El Custodio de claves entregará a la RA la clave pública en una petición de certificado en formato PKCS #10.

6.1.2. Entrega de la clave privada

- En dispositivos Hardware:

La clave privada será entregada junto al certificado en el dispositivo criptográfico portable.

La RA será responsable de garantizar la entrega del dispositivo portable al Suscriptor, asegurándose así que este último está en posesión de los datos de creación de firma o sello electrónicos (clave privada) correspondientes a los datos de validación (clave pública) que constan en el certificado.

- En dispositivo software:

La generación del certificado por el Suscriptor incluye la descarga conjunta de la clave privada y del certificado en formato PKCS #12 protegido con una contraseña que él mismo habrá establecido.

6.1.3. Entrega de la clave pública al emisor del certificado

El envío de la clave pública a la CA para la generación del certificado se realiza mediante el formato autofirmado X.509 o PKCS #10, utilizando un canal seguro para la transmisión.

6.1.4. Entrega de la clave pública de la CA a los terceros que confían en los certificados

Los certificados de la CA Raíz y la CA Subordinada de LAZZATE CIA. LTDA. y huella digital están a disposición de los usuarios en la página web de LAZZATE CIA. LTDA..

6.1.5. Tamaño de las claves

Certificado	Tamaño claves RSA (bits)	Periodo validez (años)
CA Raíz	4096	30
CA Subordinada LAZZATE CIA. LTDA.	4096	15
OCSP	2048	1
Suscriptores	2048	3 (máximo)
Operadores	2048	3 (máximo)

6.1.6. Parámetros de generación de la clave pública y verificación de la calidad

Se utilizan los parámetros recomendados en el documento de especificaciones técnicas de la ETSI TS 119 312.

Concretamente los parámetros utilizados son los siguientes:

Signature suite	Hash function	Signature algorithm
sha256-with-rsa	SHA-256	RSA-PKCSv1_5

6.1.7. Usos admitidos de la clave (campo Key Usage de X.509 v3)

Todos los certificados emitidos por la CA de LAZZATE CIA. LTDA. incluyen las extensiones Key Usage y Extended Key Usage, indicando los usos habilitados de las claves.

Los usos admitidos para los certificados de la CA Raíz y la CA Subordinada de LAZZATE CIA. LTDA. son firma de certificados y firma de CRL.

Los usos admitidos de la clave para cada tipo de certificado de Suscriptores están definidos en la Política de Certificación correspondiente.

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

6.2.1. Estándares para los módulos criptográficos

Los módulos criptográficos empleados para generar y proteger las claves de las Autoridades de Certificación (HSM) están certificados con la norma FIPS-140-2 nivel 3.

Las claves de los Suscriptores cualificados en DSCF son generadas de forma segura en un dispositivo cualificado son generadas por el propio interesado de forma segura utilizando un dispositivo criptográfico CC EAL4+, FIPS 140-1 nivel 3, ITSEC E4 High u otro de nivel equivalente.

Las claves de los Suscriptores en otros dispositivos del tipo dispositivo criptográfico portable son generadas de forma segura en un dispositivo criptográfico con certificación FIPS 140-2 nivel 2 o superior o Common Criteria EAL4+ o superior.

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

El acceso a la clave privada de la CA Raíz requiere la participación simultánea de las siguientes personas autorizadas según los roles de confianza, con uso de sus respectivos dispositivos criptográficos protegidos con un PIN:

- 3 de 5 determinadas personas, sin uso de uno de los HSM que custodian la clave privada de la CA Raíz.

- 3 de 5 determinadas personas, con uso de uno de los HSM que custodian la clave privada de la CA Raíz.

El acceso a la clave privada de la CA Subordinada de LAZZATE CIA. LTDA. requiere la participación simultánea de las siguientes personas autorizadas según los roles de confianza, con uso desus respectivos dispositivos criptográficos protegidos con un PIN:

- 3 de 5 determinadas personas, sin uso de uno de los HSM que custodian la clave privada de la CA Subordinada de LAZZATE CIA. LTDA..

- 3 de 5 determinadas personas, con uso de uno de los HSM que custodian la clave privada de la CA Subordinada de LAZZATE CIA. LTDA..

6.2.3. Custodia de la clave privada

La clave privada de la CA Raíz está custodiada por dispositivos criptográficos hardware (HSM) certificados con la norma FIPS 140-2 nivel 3, garantizando que la clave privada nunca está en claro fuera del dispositivo criptográfico. La activación y uso de la clave privada requiere el control multi persona detallado en el apartado 6.2.2. Con posterioridad a la operación realizada, la sesión se cierra, quedando desactivada la clave privada.

La clave privada de la CA Subordinada de LAZZATE CIA. LTDA. está custodiada por dispositivos criptográficos hardware (HSM) certificados con la norma FIPS 140-2 nivel 3, garantizando que la clave privada nunca está en claro fuera del dispositivo criptográfico. La activación dela clave privada requiere el control multipersona detallado en el apartado 6.2.2.

6.2.4. Copia de seguridad de la clave privada

Las claves privadas de la CA Raíz y la CA Subordinada de LAZZATE CIA. LTDA. pueden ser restauradas mediante un procedimiento de consenso entre el personal designado para el la custodia de las tarjetas criptográficas de restauración

Todas las claves internas del sistema como de los usuarios son almacenadas de forma segura dentro de los dispositivos criptográficos con el fin de ser recuperadas con una duración máxima de 10 años

6.2.5. Archivo de la clave privada

EL ECIL no archivará la clave privada de la CA Raíz después de la expiración de todos los certificados que contienen la correspondiente clave pública.

LAZZATE CIA. LTDA. no archivarán la clave privada de la CA Subordinada de LAZZATE CIA. LTDA. después de la expiración o la revocación de todos los certificados emitidos por la CA Raíz que contienen la correspondiente clave pública.

6.2.6. Almacenamiento de la clave privada en un módulo criptográfico

Existen documentos de ceremonia de claves de la CA Raíz y la CA Subordinada de LAZZATE CIA. LTDA. donde se describen los procesos de generación y almacenamiento de sus claves privadas por los módulos criptográficos empleados (HSM).

6.2.7. Método de activación de la clave privada

- La clave privada de la CA Raíz se activa en sus HSM por un proceso que requiere la utilización de 3 de 5 dispositivos criptográficos, los cuales, junto a sus respectivos PIN, constituyen, por tanto, los datos de activación de la clave privada.
- La clave privada de la CA Subordinada de LAZZATE CIA. LTDA. se activa en sus HSM por un proceso que requiere la utilización de 3 de 5 dispositivos criptográficos, los cuales, junto a sus respectivos PIN, constituyen, por tanto, los datos de activación de la clave privada.

6.2.8. Método de desactivación de la clave privada

- La clave privada de la CA Raíz se desactivará en sus HSM después de su uso, por procedimiento.
- La clave privada de la CA Subordinada de LAZZATE CIA. LTDA. sólo se desactivará en sus HSM en situaciones extraordinarias.
- La clave privada del Suscriptor con DSCF quedará desactivada una vez quese retire el dispositivo criptográfico de creación de firma o sello electrónicosdel dispositivo de lectura.

6.2.9. Método de destrucción de la clave privada

La destrucción de la clave privada de la CA Raíz o la CA Subordinada de LAZZATE CIA.

LTDA. se realiza, de acuerdo con un procedimiento documentado de destrucción de claves, por personal autorizado según los roles de confianza.

Se realizará un borrado seguro de la clave privada de la CA, utilizando las funciones que proveen los dispositivos criptográficos hardware empleados (HSM), de forma que no resulten afectadas el resto de las claves gestionadas por los dispositivos.

Asimismo, se realizará un borrado seguro de todas las copias de seguridad de la clave privada de la CA, las cuales habrán sido identificadas por el ECIL.

6.3. Otros aspectos de la gestión del par de claves

6.3.1. Archivo de la clave pública

Los certificados emitidos por la CA Subordinada de LAZZATE CIA. LTDA., y por tanto las claves públicas, se conservarán durante lo que establece la legislación que se encuentre vigente.

6.3.2. Periodo operativo de los certificados y periodo de uso del par de claves

El periodo operativo de un certificado estará determinado por el periodo de validez o por la revocación del certificado.

La clave privada no debe ser usada después del periodo de validez o la revocación del certificado.

La clave pública no debe ser usada después del periodo de validez o la revocación del certificado, excepto por los terceros que confían en los certificados para verificar datos históricos.

6.4. Datos de activación

6.4.1. Generación e instalación de los datos de activación

- Los datos de activación fueron generados de forma segura durante la ceremonia de claves.
- Los datos de activación de la clave privada del Suscriptor en DSCF son generados en el momento de inicialización del dispositivo.

Si la inicialización se produce en una entidad externa, los datos de activación le serán entregados mediante un proceso que asegure laconfidencialidad de estos ante terceros.

6.4.2. Protección de los datos de activación

Sólo el personal autorizado tiene acceso/conocimiento a/de los datos de activación de las claves privadas de la CA Raíz y la CA Subordinada de LAZZATE CIA. LTDA..

Para los certificados de los Suscriptores, una vez se ha hecho entrega del dispositivo y/o de

los datos de activación de la clave privada, es responsabilidad del Suscriptor mantener la confidencialidad de estos datos.

6.5. Controles de seguridad informática

LAZZATE CIA. LTDA. emplean sistemas fiables y productos comerciales para ofrecer los servicios como Ente de Certificación de la Información y Servicios Relacionados.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de LAZZATE CIA. LTDA. en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de usuarios y permisos.
- Configuración de eventos de log.
- Plan de backup y recuperación.
- En su caso, configuración de antivirus.
- Requerimientos de tráfico de red.

La documentación técnica y de configuración de LAZZATE CIA. LTDA. detalla la arquitectura de los equipos que ofrecen el servicio de certificación tanto en su seguridad física como lógica.

6.5.1. Requerimientos técnicos de seguridad específicos

Cada servidor de las plataformas de las CA o las RA incluye las siguientes funcionalidades:

- Control de acceso a los servicios de la CA o las RA y gestión de privilegios.
- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial del Suscriptor, las CA y las RA, y datos de auditoría.
- Auditoría de eventos relativos a la seguridad.
- Auto-diagnóstico de seguridad relacionado con los servicios de la CA y las RA.
- Mecanismos de recuperación de claves y del sistema de las CA y las RA.
- Monitoreo remoto ante fallos.

Las funcionalidades expuestas son provistas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

6.5.2. Evaluación de la seguridad informática

La seguridad de los equipos viene reflejada por un análisis de riesgos iniciales de tal forma que las medidas de seguridad implantadas son respuesta a la probabilidad e impacto producido cuando un grupo de amenazas definidas puedan aprovechar brechas de seguridad.

La seguridad física está garantizada por las instalaciones ya definidas anteriormente y la gestión de personal es fácil debido al reducido número de personas que realizan sus trabajos en los centros de datos LAZZATE CIA. LTDA. y sus proveedores.

6.6. Controles de seguridad del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

Las plataformas de las CA y las RA poseen un procedimiento de control de cambios en las versiones de sistemas operativos y aplicaciones que impliquen una mejora en sus funciones de seguridad o que corrijan cualquier vulnerabilidad detectada.

6.6.2. Controles de gestión de seguridad

6.6.2.1 Gestión de seguridad

LAZZATE CIA. LTDA. desarrollan las actividades precisas para la formación y concienciación de los empleados en materia de seguridad.

LAZZATE CIA. LTDA. exigen, mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

6.6.2.2 Clasificación y gestión de información y bienes

LAZZATE CIA. LTDA. mantienen un inventario de activos y documentación, y un procedimiento para garantizar el correcto uso y gestión de este material.

LAZZATE CIA. LTDA. disponen de procedimientos documentados de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: PÚBLICO, INTERNO y CONFIDENCIAL.

6.6.2.3 Operaciones de gestión

La CA de LAZZATE CIA. LTDA. disponen de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos. En la documentación técnica de LAZZATE CIA. LTDA. y de procedimientos de los respectivos CPD se desarrolla en detalle el proceso de gestión de incidencias.

El ECIL dispone de cajas de seguridad ignífugas para el almacenamiento desoportes físicos.

LAZZATE CIA. LTDA. tienen documentado todo el procedimiento relativo a las funciones y

responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

6.6.2.4 Tratamiento de los soportes y seguridad

Todos los soportes serán tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

6.6.2.5 Planificación del sistema

El equipo técnico de LAZZATE CIA. LTDA. mantienen un registro de las capacidades de los equipos. Juntamente con la aplicación de control de recursos de cada sistema, se puede prever un posible redimensionamiento.

6.6.2.6 Reportes de incidencias y respuesta

LAZZATE CIA. LTDA. disponen de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

6.6.2.7 Procedimientos operacionales y responsabilidades

LAZZATE CIA. LTDA. definen actividades asignadas a personas con un rol de confianza distinto, para las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

6.6.2.8 Gestión del sistema de acceso

LAZZATE CIA. LTDA. realizan todos los esfuerzos que razonablemente están a su alcance para confirmar que el acceso al sistema está limitado a las personas autorizadas. En particular:

a) Gestión general de las CA y las RA:

Se dispone de controles basados en firewalls en alta disponibilidad.

Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con autenticación fuerte.

Se dispone de procedimientos documentados de gestión de altas y bajas de usuarios y política de acceso.

Se dispone de un procedimiento para asegurar que las operaciones se realizan respetando los roles establecidos.

Cada persona tiene asociado su identificador para realizar las operaciones de certificación según su rol.

El personal será responsable de sus actos, por ejemplo, por retener logs de eventos.

b) Generación del certificado:

Las instalaciones están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y/o irregular.

La autenticación para realizar el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de las CA.

c) Gestión de la revocación:

Las instalaciones de las plataformas de las CA y las RA están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y/o irregular al sistema de revocaciones.

La revocación se refiere a la pérdida de efectividad de un certificado de forma permanente. La revocación se realizará mediante autenticación por certificado a las aplicaciones por un operador autorizado (responsable de revocación). Los sistemas de log generarán las pruebas que garantizan el no repudio de la acción realizada por el operador de CA.

d) Estado de la revocación:

La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación por certificado para evitar el intento de modificación de la información del estado de la revocación.

6.6.2.9 Gestión del ciclo de vida del hardware criptográfico de las CA

El ECIL se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte.

El hardware criptográfico está construido sobre soportes preparados para evitar cualquier manipulación.

El ECIL registra toda la información pertinente de los dispositivos para añadir al catálogo de activos de LAZZATE CIA. LTDA.

El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

EL ECIL realiza pruebas periódicas para asegurar el correcto funcionamiento de los dispositivos.

Los dispositivos criptográficos solo son manipulados por personal confiable.

Las claves privadas de firma de las CA almacenadas en el hardware criptográfico se eliminarán una vez que se hayan retirado los dispositivos.

La configuración del sistema de las CA así como sus modificaciones y actualizaciones son documentadas y controladas.

LAZZATE CIA. LTDA. posee un contrato de mantenimiento de los dispositivos para su correcto mantenimiento. Estas configuraciones se realizarán al menos por dos personas confiable.

6.7. Controles de seguridad de la red

LAZZATE CIA. LTDA. protegen el acceso físico a los dispositivos de gestión de red y disponen de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad creando secciones de red claramente definidas. Esta división esta administrada y gestionada por firewalls.

6.8. Fuente de tiempo

En el caso de las plataformas de la CA, el tiempo se obtiene mediante un hardware específico con reloj atómico de átomo de rubidio, sincronización GPS y consulta al Instituto Oceanográfico y Antártico de la Armada "INOCAR" (http://inocar.ntp.ec/), siguiendo el protocolo NTP a través de Internet. La descripción del protocolo NTP se puede encontrar en la RFC 5905 "Network Time Protocol".

7. Perfiles de los certificados, CRL y OCSP

7.1. Perfil de los certificados

El perfil de los certificados se corresponde con el propuesto en las políticas de certificación correspondientes, y son coherentes con lo dispuesto en las normas siguientes:

- ETSI EN 319 412 conocida como "European profiles for Qualified Certificates"
- 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"

El perfil común a todos los certificados es el siguiente:

Campo del certificado	Nombre	Descripción
Version	N° de versión	V3 (versión del estándar X.509)
Serial Number	N° de serie	*Código único con respecto al nombre distinguido del emisor*
Issuer	Emisor	*DN de la CA que emite el certificado*
notBefore	Válido desde	*Fecha de inicio de validez, tiempo UTC*
notAfter	Válido hasta	*Fecha de fin de validez, tiempo UTC*
Subject	Asunto (DN)	*Nombre distinguido del Firmante o Creador del sello o de la CA*

7.1.1. Número de versión

Los certificados siguen el estándar de certificados X.509 versión 3.

7.1.2. Extensiones de los certificados

Extensión	Crítica	Posibles Valores
X509v3 Subject Alternative Name	-	En el caso de certificados de usuario: rfc822Name: *email del Firmante o Creador del sello* En el caso de certificados de usuario de firma electrónica: directoryName: 1.3.6.1.4.1.59382.2.1: *Nombre de pila del Firmante* 1.3.6.1.4.1.59382.2.2: *Primer apellido del Firmante* 1.3.6.1.4.1.59382.2.3: *Segundo apellido del Firmante(este campo puede estar vacío)*
X509v3 Basic Constraints	Sí	2 valores posibles en función de si se trata de un certificado de CA o de usuario: CA: FALSE CA: TRUE
X509v3 Key Usage	Sí	En el caso de certificados de usuario: Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage	-	En el caso de certificados de usuario: TLS Web Client Authentication E-mail Protection
X509v3 Subject Key Identifier	-	*<id de la clave pública del certificado, obtenido a partir del hash de la misma>*
X509v3 Authority Key Identifier	-	*<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>*
X509v3 Authority Information Access	-	Access Method: id-ad-ocsp Access Location: *<URI de acceso al servicio OCSP>* Access Method: id-ad-calssuers Access Location: *<URI de acceso al certificado de la CA emisora>*
X509v3 CRL Distribution Points	-	*<URI de la CRL>*

X509v3 Certificate Policies	-	*<OID de la política de certificación propia de LAZZATE CIA. LTDA. correspondiente al certificado>* *<URI de la DPC>* User Notice: *<Nota de texto que se puede desplegar en la pantalla del usuario>* Cuando sea de aplicación: *<OID de la política europea>*

Las extensiones aquí presentadas se corresponden con todas las que pueden contener los certificados emitidos. En la política de certificación de cada tipo de certificado se especificará las extensiones requeridas.

Faltan todas las OIDS de políticas y tipos de certificados como en Security Data pg 68 y 69

7.1.3. Identificadores de objeto (OID) de los algoritmos utilizados

OID	Nombre	Descripción
1.2.840.113549.1.1.11	sha256WithRSAEncryption	OID del algoritmo de firma
1.2.840.113549.1.1.1	rsaEncryption	OID de Clave pública

7.1.4. Formatos de nombres

		Cuando sea de aplicación: *<OID de la política española (de empleado público, de representante legal, etc)>*
QcStatements	-	Existen los siguientes tipos: id-etsi-qcs-QcCompliance (a añadir cuando el certificado es cualificado) id-etsi-qcs-QcSSCD (a añadir cuando la clave privada se guarda en un DCCF o DCCS) id-etsi-qcs-QcLimitValue: límite del valor de las transacciones id-etsi-qcs-QcRetentionPeriod: indica el periodo de retención de la documentación id-etsi-qcs-QcPDS: URI con documento PDS, obligatorio en lengua inglesa y opcional en otras lenguas id-etsi-qcs-QcType: indica el tipo de certificado: • id-etsi-qct-esign, es un certificado de firma electrónica • id-etsi-qct-eseal, es un certificado de sello electrónico

Los siguientes atributos del DN son comunes a todos los certificados de firma electrónica.

Atributo del DN	Nombre	Descripción
CN, Common Name	Nombre	*Nombre y apellidos del Firmante*
C, Country	País	*Código de dos letras según ISO 3166-1 del país emisor del código identificativo del Firmante*
Serial Number	Número de serie	*Código identificativo del Firmante, codificado según ETSI EN 319 412-1 con uno de los tipos siguientes: IDC (national identity card number, por ejemplo, DNI en España o Perú), PNO (national personal number, por ejemplo, NIE u otro tipo de NIF distinto de DNI en España, Nº Carné de Extranjería en Perú), PAS (passport number, Nº Pasaporte)* *Ejemplo:* IDCES-00000000G
SN, Surname	Apellidos	*Apellidos (o primer apellido) del Firmante*
G, Given Name	Nombre de pila	*Nombre de pila del Firmante*

7.1.5. Restricciones de los nombres

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).

7.2. Perfil de CRL

El perfil de las CRL se corresponde con el perfil estándar de CRL X.509 de la RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". Las CRL son firmadas por la CA que ha emitido los certificados.

7.2.1. Número de versión

Las CRL emitidas por la CA siguen el estándar de CRL X.509 versión 3.

7.2.2. CRL y extensiones

7.2.2.1 CRL de la CA Raíz de El ECI LAZZATE CIA. LTDA. (ARL)

CAMPOS	VALORES
Versión	V2 (versión del estándar X.509)
Número de CRL	*Número incremental*
Algoritmo de firma	sha256WithRSAEncryption
Emisor (Issuer)	Distinguished Name (DN) del emisor

Fecha efectiva de emisión	*Fecha de emisión de la CRL, tiempo UTC*
Fecha de próxima actualización	*Fecha de emisión* + 6 meses
Identificador de la clave de autoridad	Hash de la clave del emisor
Sólo contiene Certificados de usuario	NO
Sólo contiene Certificados de la entidad emisora	NO
Lista de certificados revocados (CRL) indirecta	NO
Entradas de la CRL	*Nº de serie del certificado Fecha de revocación Código de razón*

7.2.2.2 CRL de la CA Subordinada de LAZZATE CIA. LTDA.

CAMPOS	VALORES
Versión	V2 (versión del estándar X.509)
Número de CRL	*Número incremental*
Algoritmo de firma	sha256WithRSAEncryption
Emisor (Issuer)	Distinguished Name (DN) del emisor
Fecha efectiva de emisión	*Fecha de emisión de la CRL, tiempo UTC*
Fecha de próxima actualización	*Fecha de emisión* + 7 días
Identificador de la clave de autoridad	Hash de la clave del emisor
Sólo contiene Certificados de usuario	NO
Sólo contiene Certificados de la entidad emisora	NO
Lista de certificados revocados (CRL) indirecta	NO
Entradas de la CRL	*Nº de serie del certificado Fecha de revocación Código de razón*

7.3. Perfil de OCSP

El Servicio de Validación de Certificados se basa en el uso del protocolo OCSP sobre HTTP, definido en la norma RFC 6960 “En línea Certificate Status Protocol – OCSP”.

Los servicios de OCSP cumplen con la norma IETF RFC 6960.

8. Auditorías de cumplimiento y otros controles

8.1. Frecuencia de las auditorías

Se realizarán auditorías periódicas necesarias, con un intervalo de 30 días. Estas auditorias serán de carácter interno.

8.2. Cualificación del auditor

Las auditorías pueden ser de carácter tanto interno como externo. En este segundo caso, se realizan por empresas que sean reconocidas local y mundial por su experticia en el ámbito requerido.

8.3. Relación entre el auditor y la entidad auditada

Las empresas que realizan las auditorías externas nunca presentan conflictos de intereses que puedan desvirtuar su actuación en su relación con LAZZATE CIA. LTDA..

8.4. Aspectos cubiertos por los controles

Las auditorías verifican los siguientes principios:

a) Publicación de la información. El ECIL hace públicas las prácticas de negocio y de gestión de certificados (la presente DPC), así como la política de privacidad de la información y protección de datos personales y proporciona sus servicios en conformidad con dichas prácticas y política.

b) Integridad de servicio. El ECIL mantiene controles efectivos para asegurar razonablemente que:

La información del Suscriptor, del Solicitante, y del Firmante o del Custodio de claves es identificada y autenticada adecuadamente (para las actividades de registro realizadas por las RA).

Se mantiene la integridad de las claves y certificados gestionados y su protección a lo largo de todo su ciclo de vida.

c) Controles generales. El ECIL mantiene controles efectivos para asegurar razonablemente que:

La información de los Suscriptores está restringida a personal autorizado y protegida de usos no especificados en las prácticas de negocio del ECIL publicadas.

Se mantiene la continuidad de las operaciones relativas a la gestión del ciclo devida de las claves y los certificados.

Las tareas de explotación, desarrollo y mantenimiento de los sistemas del ECIL son adecuadamente autorizadas y realizadas para mantener la integridad de estos.

8.4.1. Auditorías en las Autoridades de Registro

Las Autoridades de Registro que tengan acceso al software para la gestión de certificados son auditadas por LAZZATE CIA. LTDA. o por un tercero designado por LAZZATE CIA. LTDA. previamente a su puesta en marcha efectiva.

Adicionalmente, se realizan auditorías que comprueban el cumplimiento de los requerimientos exigidos por las Políticas de Certificación para el desarrollo de las labores de registro expuestas en el contrato de servicio firmado.

La periodicidad de las auditorías vendrá determinada por el acuerdo entre LAZZATE CIA. LTDA. y la Autoridad de Registro, siempre teniendo en cuenta la actividad prevista a desarrollar por la Autoridad de Registro en cuanto a número de certificados o requerimientos específicos de seguridad.

No obstante, y excepcionalmente, LAZZATE CIA. LTDA. podría eximir a una Autoridad de Registro de la obligación de someterse a una auditoría inicial y a las auditorías de mantenimiento.

8.5. Acciones para emprender como resultado de la detección de incidencias

En caso de que sean detectadas incidencias o no-conformidades, se tomarán las medidas oportunas para su resolución en el menor tiempo posible. Para no-conformidades graves (que afectan a los servicios críticos, a saber, servicios de revocación y servicios de publicación de CRL), LAZZATE CIA. LTDA. se comprometen a su resolución en un plazo máximo de 30 días.

En todo caso se formará un comité de resolución formado por personal de las áreas afectadas y otro de seguimiento formado por los responsables de las áreas afectadas y el Responsable de Seguridad de LAZZATE CIA. LTDA..

8.6. Comunicación de resultados

El auditor comunicará los resultados al Responsable de Seguridad y/o al representante de la Dirección de LAZZATE CIA. LTDA..

9. Otros asuntos legales y de actividad

9.1. Tarifas

9.1.1. Tarifas de emisión de certificado o renovación

Los precios de los servicios de certificación estarán detallados para consulta de los clientes o

posibles clientes por el Departamento Comercial de LAZZATE CIA. LTDA. o por la RA, así como en su portal web u otros medios contemplados como canales comerciales del ECIL.

9.1.2. Tarifas de acceso a los certificados

El acceso a los certificados emitidos por los respectivos Suscriptores, y Firmantes o Custodios de claves es gratuito.

Los precios están sujetos a variaciones y modificaciones que dependen o no de normativas vigentes en el país, así como de promociones o descuentos ofertados sobre nuestros servicios y productos. Estas modificaciones pueden ser sin previo aviso, y estas serán comunicadas por todos los canales de información de la ECIL.

9.1.3. Tarifas de revocación o acceso a la información del estado

No se establece ninguna tarifa para la revocación de certificados.

LAZZATE CIA. LTDA. provee un acceso gratuito a la información relativa al estado de los certificados, por medio de la publicación de las correspondientes CRL y del servicio OCSP.

LAZZATE CIA. LTDA. puede ofrecer otros servicios de validación de certificados comerciales, cuyas tarifas serán negociadas con cada cliente de estos servicios.

9.1.4. Tarifas de otros servicios

Las tarifas aplicables a otros servicios se negociarán entre LAZZATE CIA. LTDA. y los clientes de los servicios ofrecidos.

9.1.5. Devoluciones y reembolsos

Los clientes podrán aplicar a la devolución o reembolso del pago efectuado por concepto de la suscripción, bajo los siguientes casos:

- Duplicidad en el pago mediante tarjeta de débito o crédito.
- Pago en exceso.
- Si el producto o servicio no fue proporcionado y el suscriptor desea abandonar el trámite.

Para tal efecto, el cliente deberá contactarse con el ECIL mediante los canales de servicio al cliente, para exponer las razones de la devolución o reembolso. Cada caso será sometido a análisis donde se determinará si es aplicable la devolución o reembolso del pago.

Este no será mayor ni menor al valor pagado por el suscriptor.

9.2. Confidencialidad de la información

LAZZATE CIA. LTDA. dispone de una adecuada política de tratamiento de datos personales y de los modelos de acuerdo que deberán firmar todas las personas que tengan acceso a información confidencial, basada en la normativa vigente.

9.2.1. Ámbito de la información confidencial

LAZZATE CIA. LTDA. considerará confidencial toda la información que esté catalogada expresamente como confidencial. No se difundirá información declarada como confidencial sin el consentimiento expreso por escrito de la persona, empresa u organización que le haya otorgado el carácter de confidencial, a no ser que el requerimiento sea resultado de una solicitud judicial que guarde toda la formalidad legal.

9.2.2. Información no confidencial

La siguiente información será considerada no confidencial:

- La contenida en la presente DPC.
- La contenida en las distintas Políticas de Certificación.
- La información contenida en los certificados, puesto que para su emisión el Suscriptor y, en su caso, el Firmante o el Custodio de claves otorgan previamente su consentimiento, incluyendo los diferentes estados o situaciones del certificado.
- Las listas de certificados revocados (CRL), así como las restantes informaciones de estado de revocación.
- En su caso, la información contenida en los repositorios de certificados.
- Cualquier otra información cuya publicidad sea impuesta normativamente.

9.2.3. Responsabilidad en la protección de información confidencial

Es responsabilidad de LAZZATE CIA. LTDA., y las RA establecer medidas adecuadas para la protección de la información confidencial.

9.3. Protección de la información personal

9.3.1. Política de protección de datos de carácter personal

En cumplimiento de los requisitos establecidos en la normativa aplicable en materia de protección de datos personales, LAZZATE CIA. LTDA. realizará el tratamiento estrictamente necesario de dichos datos con el fin de prestar los servicios de certificación contratados.

9.3.1.1 Aspectos cubiertos

El presente documento describe los procedimientos, requisitos y obligaciones en relación con la obtención y gestión de los datos de carácter personal, cumpliendo con lo establecido en la normativa aplicable en materia de protección de datos personales.

9.3.2. Información tratada como privada

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

La información personal que no haya de ser incluida en los certificados y en el mecanismo indicado de comprobación del estado de los certificados, es considerada información personal de carácter privado.

Los siguientes datos son considerados en todo caso como información privada:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en el apartado 9.3.2.
- Claves privadas generadas por la Autoridad de Certificación.
- Toda otra información identificada como privada.

En cualquier caso, los datos captados por el ECIL deberán ser tratados con el de nivel de seguridad básico.

9.3.2.1 Estructura de los ficheros de carácter personal

Ámbito personal	Nombre y apellidos
	E-mail personal
	Teléfono personal
	Domicilio personal
	País emisor del código identificativo personal
	Código identificativo personal (tipo y número)
	Titulaciones académicas (titulación y organismo emisor)
Ámbito profesional	Nombre de la organización
	Código identificativo de la persona jurídica
	Departamento en la organización
	Cargo, título o rol en la organización
	Domicilio profesional
	E-mail profesional
	Teléfono profesional

9.3.3. Información no calificada como privada

La siguiente información no está calificada como privada:

- La información contenida en los certificados, puesto que para su emisión el Suscriptor otorgan previamente su consentimiento, incluyendo los diferentes estados o situaciones del certificado.
- Las listas de certificados revocados (CRL), así como las restantes informaciones de estado de revocación.

9.4. Obligaciones

9.4.1. Obligaciones de la CA

a) Respetar lo dispuesto en las Políticas y Prácticas de Certificación (el presente

documento, las PC y la PDS).

b) Publicar esta DPC, las PC en su página Web.

c) Informar sobre las modificaciones de esta DPC a los Suscriptores y al público en general, incluyendo dichas modificaciones en la tabla inicial de historial de versiones.

d) Disponer de un seguro de responsabilidad civil que cubra el valor mínimo exigido por la normativa vigente.

e) Utilizar sistemas fiables para almacenar certificados cualificados que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el Firmante o Suscriptor haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.

f) En caso de cese de actividad, cumplir lo especificado en el apartado específico.

Por lo que a certificados respecta:

a) Emitir certificados conforme a esta DPC y a los estándares de aplicación.

b) Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos.

c) Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente, cuando sea aplicable.

d) Revocar los certificados según lo dispuesto en la DPC y publicar las mencionadas revocaciones en la CRL (Lista de Certificados Revocados) y en el servicio OCSP.

Sobre custodia de información:

a) Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente, cuando sea aplicable.

b) No almacenar ni copiar los datos de creación de firma electrónica del Suscriptor o los datos de creación de sello electrónico del Suscriptor, salvo en caso de su gestión en nombre del titular.

c) Proteger, con el debido cuidado, los datos de creación de firma electrónica del Suscripto, garantizando que se utilicen, con un alto nivel de confianza, bajo el control exclusivo del Suscriptor, así como su continua disponibilidad.

d) Proteger sus claves privadas de forma segura.

e) Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida, destrucción o falsificación.

9.4.2. Obligaciones de las RA

a) Respetar lo dispuesto en esta DPC y en las PC correspondientes a los tipos de

certificados que emitan.

b) Respetar lo dispuesto en los contratos firmados con la CA.

c) Respetar lo dispuesto en los contratos firmados con el Suscriptor. En el ciclo de vida de los certificados:
a) Comprobar la identidad de los Suscriptores según lo descrito en esta DPC o mediante otro procedimiento que haya sido aprobado por LAZZATE CIA. LTDA..

b) Verificar la exactitud y autenticidad de la información suministrada por el Solicitante, y el Firmante o el Custodio de claves.

c) Informar al Solicitante antes de la emisión de un certificado, de las obligaciones que asume, la forma en la que debe custodiar los datos o dispositivos de creación de firma electrónica o sello electrónico y/o los datos de acceso a los mismos, el procedimiento que debe seguir para comunicar la pérdida o utilización indebida de los datos o dispositivos de creación de firma electrónica o sello electrónico, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad patrimonial, y de la página web donde puede consultar cualquier información de LAZZATE CIA. LTDA., de la DPC y de la PC correspondiente al certificado.

d) Tramitar y entregar los certificados conforme a lo estipulado en esta DPC y en la PC correspondiente.

e) Formalizar los documentos contractuales con el Suscriptor según lo establecido en la Política de Certificación aplicable.

f) Abonar las tarifas establecidas por los servicios de certificación solicitados.

g) Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el Suscriptor.

h) Informar a la CA de las causas de revocación, siempre y cuando tengan conocimiento de estas.

i) Realizar las comunicaciones con los Suscriptores, por los medios que consideren adecuados, para correcta gestión del ciclo de vida de los certificados. Concretamente realizar las comunicaciones relativas a la proximidad de la caducidad de los certificados y a las revocaciones de estos.

9.4.3. Obligaciones de los Suscriptores

a) Suministrar a la RA la información necesaria para realizar una correcta identificación.

b) Dar cumplimiento obligatorio a toda la normativa que fuese emitida por la Entidad de Certificación LAZZATE CIA. LTDA.

c) Realizar los esfuerzos que razonablemente estén a su alcance para confirmar la exactitud y veracidad de la información suministrada.

d) Respetar lo dispuesto en los documentos contractuales firmados con la CA y la RA.

e) Notificar a el ECIL cualquier cambio en los datos aportados para la creación del certificado de firma electrónica durante su periodo de validez.

f) Informar a la mayor brevedad posible de la existencia de alguna causa derevocación.

g) Responsabilizarse por el uso del Certificado de Firma Electrónica y de las implicaciones que resulten del uso indebido de este.

h) Resguardar de forma segura el contenedor hardware (token).

i) Cumplir con la normativa vigente sobre la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, y el Art. 17 de dicha Ley.

9.4.4. Obligaciones de los terceros que confían en los certificados

a) Verificar la vigencia de los certificados antes de realizar cualquier operación basadaen los mismos, lo cual incluirá comprobar que los certificados no han expirado ni han sido revocados (mediante consulta de la CRL).

b) Verificar que los certificados han sido firmados con la clave privada asociada a un certificado vigente de la CA Subordinada de LAZZATE CIA. LTDA..

c) Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía.

9.5. Exención de garantía

LAZZATE CIA. LTDA. puede rechazar toda garantía de servicio que no se encuentre vinculado a las obligaciones establecidas por la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

9.6. Responsabilidades

9.6.1. Responsabilidades de la Autoridad de Certificación

LAZZATE CIA. LTDA., garantiza el cumplimento de la normativa, obligaciones y responsabilidades que se estipulan en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, así como las descritas en esta DPC.

a) Garantizar el cumplimiento de las responsabilidades y obligaciones descritas en esta DPC; y lo previsto en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos, y su Reglamento.

b) El ECIL, única y exclusivamente, responderá por daños y perjuicios que causen a cualquier persona, cuando incumpla sus obligaciones legales derivadas de la legislación vigente en la República del Ecuador o cuando actúe con la negligencia en la prestación de servicios de certificación.

c) El ECIL, no será responsable de los daños derivados de o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo del Solicitante, Suscriptor y/o Usuario.

d) El ECIL, no será responsable de la utilización negligente o dolosa de los certificados y las claves.

e) El ECIL, no será responsable de los daños y perjuicios que se deriven de actuaciones negligentes o dolosas por parte de terceros con relación a los certificados por ella emitidos a favor de un determinado suscriptor.

f) El ECIL, no será responsable de las eventuales inexactitudes en el Certificado que resulten de la información facilitada por el Suscriptor, a condición de haber actuado siempre con la máxima negligencia exigible.

g) El ECIL, no será responsable de los daños que se deriven de aquellas operaciones en que se hayan incumplido las limitaciones de uso que se señalan en las políticas de certificación correspondientes a cada tipo de certificado.

h) El ECIL, no asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones en virtud de la presente DPC si tal falta de ejecución o retraso resultara o fuera consecuencia de un supuesto de fuerza mayor, caso fortuito o, en general, cualquier circunstancia sobre la que La ECIL, no pueda tener un control razonable.

i) El ECIL, no será responsable del contenido de aquellos documentos electrónicos firmados digitalmente. Ni La ECIL, ni sus autoridades de registro serán responsables en ningún caso por los daños causados por el empleo de sus servicios de certificación pública en estos entornos.

9.6.2. Responsabilidades de la Autoridad de Registro

La RA asumirá toda la responsabilidad en el procedimiento de identificación y autenticación de los Suscriptores, y de los Firmantes. Deberá para ello proceder según lo estipulado en la presente DPC o según otro procedimiento aprobado por LAZZATE CIA. LTDA..

Si la generación del par de claves no se realiza en presencia del Firmante, la RA será responsable de la custodia de las claves hasta su entrega al Custodio de claves.

9.6.3. Responsabilidades del Suscriptor

a) El Suscriptor será responsable por los daños y perjuicios causados por el incumplimiento de sus respectivas obligaciones enumeradas en esta DPC.

b) El Suscriptor será responsable del cumplimiento de todas aquellas obligaciones impuestas por la presente DPC, las PC de cada tipo de Certificado, y por la normativa vigente en materia de prestación de servicios de certificación.

c) El Suscriptor se compromete a indemnizar a él EC LAZZATE CIA. LTDA. los daños o perjuicios que puedan ocasionar cualquier acto u omisión culposa o dolosa de su parte, asumiendo igualmente los costos procesales en que el EC LAZZATE CIA. LTDA. pudiera incurrir por esta causa, incluyendo los honorarios profesionales de Abogados y

Procuradores.

d) El Suscriptor indemnizará y mantendrá indemne a él EC LAZZATE CIA. LTDA. por cualquier daño que esta pudiera sufrir por el cumplimiento total, parcial o defectuoso de las obligaciones asumidas ye en base a toda reclamación dirigida contra ella por cualquier tercero con lo que el suscriptor hubiera contratado.

9.6.4. Responsabilidades del Usuario

a) El Usuario será responsable por los daños y perjuicios causados por el incumplimiento de sus respectivas obligaciones enumeradas en esta DPC.

b) El Usuario será responsable del cumplimiento de todas aquellas obligaciones impuesta por la presente DPC, las PC de cada tipo de Certificado, y por la normativa vigente en materia de prestación de servicios de certificación.

c) En todo caso, el Usuario asumirá toda la responsabilidad y riesgos derivados de la aceptación de un Certificado sin haber observado las obligaciones recogidas en la DPC y, en su caso, en las PC específicas de cada certificado, garantizando la plena indemnidad de la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL por dicho concepto.

9.7. Periodo de validez

9.7.1. Plazo

La DPC, la PDS y las PC entran en vigor en el momento de su publicación en la web de LAZZATE CIA. LTDA..

9.7.2. Sustitución y derogación de la DPC

La presente DPC, la PDS y las PC serán derogadas en el momento en que una nueva versión del documento sea publicada en la web de LAZZATE CIA. LTDA..

La nueva versión sustituirá íntegramente el documento anterior.

9.7.3. Efectos de la finalización

Para los certificados vigentes emitidos bajo una DPC o PC anterior, la nueva versión prevalecerá a la anterior en todo lo que no se oponga a ésta.

ENTE CERTIFICACIÓN
FIRMA ELECTRÓNICA
LAZZATE - ENEXT