INDICE

1. INTRODUCCIÓN

1.1. PRESENTACIÓN

La presente Declaración de Prácticas de Certificación (DPC) constituye el marco normativo y operativo fundamental que rige la prestación de servicios de certificación por parte de Eclipsoft S.A. en su calidad de Entidad de Certificación de Información y Servicios Relacionados acreditada por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL).

Esta DPC describe detalladamente condiciones, políticas y procedimientos aplicables a la solicitud, emisión, uso, suspensión y revocación de los certificados de firma electrónica, así como la operación de los servicios de sellado de tiempo, en el territorio de la República del Ecuador.

1.2. DESCRIPCION GENERAL

Somos una Autoridad de Certificación acreditada por ARCOTEL dedicada a otorgar seguridad jurídica y fiabilidad técnica a las transacciones electrónicas, nuestra actuación se fundamenta en el estricto cumplimiento de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley Nº 2002-67, publicada en el Registro Oficial Suplemento 557, 17-IV-2002), el Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Decreto ejecutivo 3496, publicado en el Registro Oficial 735, 31-XII-2002), Ley Orgánica de Protección de Datos Personales y su reglamento vigente y la Resolución ARCOTEL-2024-0176 en la cual se expide la Norma técnica para la Prestación de los servicios de información y servicios relacionados de las entidades de certificación acreditadas y terceros vinculados suscrita el 16 de agosto del 2024.

Operamos con una infraestructura certificada en sitios seguros, implementamos estrictos controles de acceso y confidencialidad en la generación de claves, y mantenemos una política de transparencia activa mediante la publicación de nuestras prácticas de certificación y el reporte periódico al organismo regulador, garantizando

así la integridad y validez legal de los certificados emitidos para nuestros suscriptores y partes usuarias.

Los certificados que se emiten a través de la Entidad de Certificación acreditada son los siguientes:

- **De Persona natural**
  - Certificado de Persona Natural en archivo
  - Certificado de Persona Natural en Dispositivo seguro de creación de firma - DSCF

- **De Persona Natural o Física - Miembro de Empresa o En Relación de Dependencia**
  - Certificado de Miembro de Empresa o Relación de Dependencia en archivo
  - Certificado de Miembro de Empresa o en Relación de Dependencia en Dispositivo seguro de creación de firma - DSCF

- **De Representante Legal**
  - Certificado de Representante Legal en archivo
  - Certificado de Representante Legal en Dispositivo seguro de creación de firma - DSCF

- **De Sello electrónico**
  - Certificado de Sello Electrónico en Archivo
  - Certificado de Sello Electrónico en Dispositivo seguro de creación de firma - DSCF

- **De Sello de Tiempo**
  - Certificado de sellado de tiempo

1.3. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

Para un riguroso control documental y transparencia, la presente DPC se identifica de la siguiente manera:

Campo:	Valor
Título del Documento:	Declaración de Prácticas de Certificación (DPC)
Versión:	3.0
OID del Documento:	1.3.6.1.4.1.57153.1.1
Fecha de Aprobación:	16 de abril de 2026
Fecha de Publicación en Repositorio:	17 de abril de 2026
Estado:	Vigente
Ubicación de Publicación (URL):	https://firmas.eclipsoft.com/dpc/

La presente DPC se mantiene disponible para consulta pública en el repositorio institucional de ECLIPSOFT, a través del enlace antes señalado, en su versión vigente.

CONTROL DE VERSIONES

VERSIÓN:	FECHA:	DETALLE DE CAMBIOS Y/O MODIFICACIONES	ELABORADO POR:
1.0	Original	Creación del documento	Alejandro Grande
2.0	10/12/2025	Actualización de la Jerarquía de Eclipsoft. (1.3.1) (1.3.1.1) (1.3.1.2) (4.9.8) (4.9.11) (6.1.1)	Nancy Caguana

		Se corrige la nomenclatura de los distintos perfiles de certificado para ajustarlos a la normativa técnica. (6.1.1) Actualización de las certificaciones. (1.3.4) Se añaden las obligaciones relativas a las organizaciones externas que ayudan en la provisión del servicio. (1.3.4.1) Se actualiza ejemplo con referencia a Ecuador (3.1.1.8) Se omite solicitar Lugar y Fecha de nacimiento al ser un dato personal no relevante. (3.2.2) Se modifica el apartado para incluir condiciones de emisión de un operador de RA. (3.2.5) Se agregan las causas de revocación de certificados. (4.9.1)	

		Se agregan las causas de suspensión de certificados. (4.9.2) Se modifican los apartados para precisar más detalles sobre los procedimientos de revocación, suspensión o reactivación. (4.9.5) Se indica que los sistemas de sincronización con UTC al menos una vez al día respecto a los procedimientos para la revocación de certificados de usuario final. (4.9.7) Se añaden las acciones a realizar por ECLIPSOFT en caso de que no se pueda tramitar y confirmar la petición de revocación en el período indicado. (4.9.7) Se añade la previsión respecto a la sincronización con UTC diaria de los sistemas respecto a los certificados de CA. (4.9.9) Se indican los eventos relacionados con la sincronización de las fuentes de tiempo	

		empleadas para proporcionar la precisión adecuada en la marca de tiempo de los diferentes registros, así como los relacionados con caídas y fallos del hardware, y actividades del firewall. (5.4.1) Se elimina el apartado - Copia de respaldo de la clave. (6.2.4) Se actualiza el apartado. (7.1.2) Se incluye el link a los procedimientos de resolución de disputas. (9.6.1.)	
3.0	15/04/2026	Se agrega contenido en los apartados de Introducción (1.1) (1.2) Se actualiza el apartado agregando información relevante de la DPC (1.3) Se corrige tabla de OID (1.3.1) Se corrige la gráfica de las jerarquías (1.4.1)	Nancy Caguana

		Se actualizan los OID´s de los certificados (1.5.1.1) (1.5.1.2) (1.5.1.3) (1.5.1.4) (1.5.1.5) (1.5.1.6) (1.5.1.7) (1.5.1.8) (1.5.1.9) Se especifica la información del responsable y se agrega información detallada y esencial de contacto (1.6) (1.6.1) (1.6.2) Se actualiza la descripción y se agrega detalle técnico de arquitectura (2.1) Se agrega información detallada y diferenciada de accesos, así como la publicación de los certificados (2.2) Se actualiza y detalla con precisión la frecuencia de emisión y actualización de CRL´s (2.3) Se actualiza y detalla los controles de acceso implementados (2.4) Se omite ESTADO, y se coloca LOCALITY (campo ciudad) como campo obligatorio en todos los certificados	

		(3.1.1.1) (3.1.1.2) (3.1.1.3) (3.1.1.4) (3.1.1.5) (3.1.1.6) (3.1.1.7) (3.1.1.8) (3.1.1.9) Se aclara que no generamos certificados de prueba y se agrega el detalle del entorno de pruebas (3.1.2.1) Se especifican datos técnicos de claves y certificados (4.5) Se actualiza el apartado agregando información detallada del proceso de renovación de certificados (4.6) Se actualiza procedimiento de renovación on-line (4.7.2) Se especifica información sobre la entidad evaluadora (8.2) Se especifican los 15 días hábiles de plazo para la entrega de resultados. (8.6) Se agrega el detalle y desglosado de las tarifas vigentes (9.1) Se actualiza el apartado	

		(9.1.2) Se actualiza el apartado (9.1.3) Se actualizan las especificaciones relacionadas a los límites de responsabilidad económica (9.6.4)	

1.3.1. IDENTIFICADORES DE CERTIFICADOS

ECLIPSOFT ha asignado a cada política de certificado un identificador de objeto (OID), para su identificación por las aplicaciones.

CA ECLIPSOFT - JERARQUIA 2025

Número OID	Tipo de certificados
1.3.6.1.4.1.57153.2.1	**Persona Natural o Física**
1.3.6.1.4.1.57153.2.1.1	*Certificado de Persona Natural en archivo*
1.3.6.1.4.1.57153. 2.1.2	*Certificado de Persona Natural en Dispositivo seguro de creación de firma - DSCF*
1.3.6.1.4.1.57153.2.2	**Persona Natural o Física - Miembro de Empresa o En Relación de Dependencia**
1.3.6.1.4.1.57153.2.2.1	*Certificado de Miembro de Empresa o Relación de Dependencia en archivo*
1.3.6.1.4.1.57153.2.2.2	*Certificado de Miembro de Empresa o en Relación de Dependencia en Dispositivo seguro de creación de firma - DSCF*
1.3.6.1.4.1.57153. 2.3	**Representante Legal**
1.3.6.1.4.1.57153.2.3.1	*Certificado de Representante Legal en archivo*

1.3.6.1.4.1.57153.2.3.2	*Certificado de Representante Legal en Dispositivo seguro de creación de firma - DSCF*
1.3.6.1.4.1.57153.102.2.4	**Sello electrónico**
1.3.6.1.4.1.57153.102.2.4.1	*Certificado de Sello Electrónico en Archivo*
1.3.6.1.4.1.57153.102.2.4.2	*Certificado de Sello Electrónico en Dispositivo seguro de creación de firma - DSCF*
1.3.6.1.4.1.57153.102.2.5	**Sello de Tiempo**
1.3.6.1.4.1.57153.102.2.5.1	*Certificado de sello de tiempo electrónico*

CA JERARQUIA 2016

Número OID	Tipo de certificados
1.3.6.1.4.1.57153.1.1.1	**Persona Natural o Física**
1.3.6.1.4.1.57153.1.1.1.1	*Certificado de Persona Natural en archivo*
1.3.6.1.4.1.57153. 1.1.1.2	*Certificado de Persona Natural en Dispositivo seguro de creación de firma - DSCF*
1.3.6.1.4.1.57153.1.1.2	**Persona Natural o Física - Miembro de Empresa o En Relación de Dependencia**
1.3.6.1.4.1.57153. 1.1.2.1	*Certificado de Miembro de Empresa o Relación de Dependencia en archivo*
1.3.6.1.4.1.57153. 1.1.2.2	*Certificado de Miembro de Empresa o en Relación de Dependencia en Dispositivo seguro de creación de firma - DSCF*
1.3.6.1.4.1.57153. 1.1.3	**Representante Legal**
1.3.6.1.4.1.57153. 1.1.3.1	*Certificado de Representante Legal en archivo*

1.3.6.1.4.1.57153. 1.1.3.2	*Certificado de Representante Legal en Dispositivo seguro de creación de firma - DSCF*
1.3.6.1.4.1.57153. 1.1.4	**Persona Jurídica - Sello De Empresa**
1.3.6.1.4.1.57153. 1.1.4.1	*Certificado de Sello Electrónico en Archivo*
1.3.6.1.4.1.57153. 1.1.4.2	*Certificado de Sello Electrónico en Dispositivo seguro de creación de firma - DSCF*
1.3.6.1.4.1.57153.102.2.5	**Sello de Tiempo**
1.3.6.1.4.1.57153.102.2.5.2	*Certificado de sello de tiempo electrónico*

En caso de contradicción entre esta Declaración de Prácticas de Certificación y otros documentos de prácticas y procedimientos, prevalecerá lo establecido en esta Declaración de Prácticas.

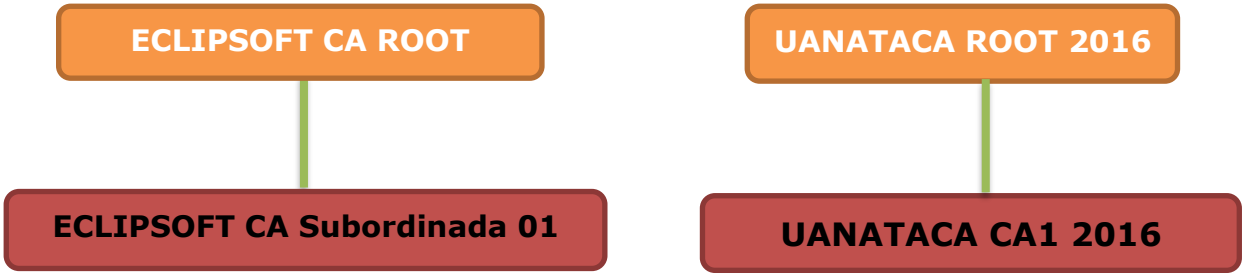
1.4. PARTICIPANTES EN LOS SERVICIOS DE CERTIFICACIÓN

1.4.1. ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN (ECI)

La Entidad de Certificación de Información (ECI) o indistintamente el prestador de servicios electrónicos de certificación es la persona, física o jurídica, que expide y gestiona certificados para entidades finales, empleando una Autoridad de Certificación, o presta otros servicios relacionados con la firma electrónica.

ECLIPSOFT es una Entidad de Certificación de Información, que actúa de acuerdo con lo dispuesto en la Ley 2002-67, Ley de comercio electrónico, firmas electrónicas y mensajes de datos, así como el Reglamento general a la ley de comercio electrónico, firmas electrónicas y mensajes de datos.

Para la prestación de los servicios de certificación, ECLIPSOFT ha establecido dos jerarquías de entidades de certificación:



1.4.1.1. ECLIPSOFT CA ROOT

Se trata de la entidad de certificación raíz de la jerarquía que emite certificados a otras entidades de certificación, y cuyo certificado de clave público ha sido auto firmado.

Datos de identificación:

CN:	ECLIPSOFT CA ROOT
Huella digital:	5f86a9f163e60ee12afce2a283399baa68f8a4c5
Válido desde:	martes, 2 de diciembre de 2025
Válido hasta:	sábado, 3 de diciembre de 2050
Longitud de clave RSA:	4096 Bits

1.4.1.2. ECLIPSOFT CA Subordinada 01

Se trata de la entidad de certificación dentro de la jerarquía que emite los certificados a las entidades finales y los certificados de sellado electrónico de tiempo, y cuyo certificado de clave pública ha sido firmado digitalmente por la ECLIPSOFT CA ROOT.

Datos de identificación:

CN:	ECLIPSOFT CA Subordinada 01
Huella digital:	fdd2d4a21efab9528ffb638203aa92d308fdfdd1
Válido desde:	martes, 2 de diciembre de 2025
Válido hasta:	jueves, 2 de diciembre de 2038
Longitud de clave RSA:	4096 Bits

1.4.1.3. UANATACA ROOT 2016

Se trata de la entidad de certificación raíz de la jerarquía que emite certificados a otras entidades de certificación, y cuyo certificado de clave público ha sido auto firmado.

Datos de identificación:

CN:	UANATACA ROOT 2016
Huella digital:	6dc08450a95cd32662c0910f8c2dce230d7466ad
Válido desde:	Viernes, 11 de marzo de 2016
Válido hasta:	Lunes, 11 de marzo de 2041
Longitud de clave RSA:	4096 Bits

1.3.1.4. UANATACA CA1 2016

Se trata de la entidad de certificación dentro de la jerarquía que emite los certificados a las entidades finales y los certificados de sellado electrónico de tiempo, y cuyo certificado de clave pública ha sido firmado digitalmente por la UANATACA CA ROOT.

Datos de identificación:

CN:	UANATACA CA1 2016
Huella digital:	7f2cb4f769224cb0cf8b692751cbd4cc64a2c450
Válido desde:	viernes, 11 de marzo de 2016
Válido hasta:	domingo, 11 de marzo de 2029
Longitud de clave RSA:	4096 Bits

1.4.2. ENTIDAD DE REGISTRO O AUTORIDAD DE REGISTRO

Una Entidad de Registro (ER) de ECLIPSOFT es la entidad encargada de:

- Tramitar las solicitudes de certificados.

- Identificar al solicitante y comprobar que cumple con los requisitos necesarios para la solicitud de los certificados.
- Validar las circunstancias personales de la persona que constará como firmante del certificado.
- Gestionar la generación de claves y la emisión del certificado
- Hacer entrega del certificado al suscriptor o de los medios para su generación.
- Custodiar la documentación relativa a la identificación y registro de los firmantes y/o suscriptores y gestión del ciclo de vida de los certificados.

Podrán actuar como ER de ECLIPSOFT:

- Cualquier entidad autorizada por ECLIPSOFT.
- ECLIPSOFT directamente.

ECLIPSOFT formalizará contractualmente las relaciones entre ella misma y cada una de las entidades que actúen como Entidad de Registro de ECLIPSOFT.

La entidad que actúe como Entidad de Registro de ECLIPSOFT podrá autorizar a una o varias personas como Operador de la ER para operar con el sistema de emisión de certificados de ECLIPSOFT en nombre de la Entidad de Registro.

La Entidad de Registro podrá delegar las funciones de identificación de los suscriptores y/o firmantes, previo acuerdo de colaboración en el que se acepte la delegación de estas funciones. ECLIPSOFT deberá autorizar de manera expresa dicho acuerdo de colaboración.

También podrán ser Entidades de Registro sujetas a esta Declaración de Prácticas de Certificación, las unidades designadas para esta función por los suscriptores de los certificados, como un departamento de personal, dado que disponen de los registros auténticos acerca de la vinculación de los firmantes con el suscriptor.

1.4.3. ENTIDADES FINALES

Las entidades finales son las personas u organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales, para los usos de autenticación y firma electrónica.

Serán entidades finales de los servicios de certificación de ECLIPSOFT las siguientes:

1. Suscriptores del servicio de certificación
2. Firmantes
3. Partes usuarias

1.4.3.1. SUSCRIPTORES DEL SERVICIO DE CERTIFICACIÓN

Los suscriptores del servicio de certificación son:

- Las empresas, entidades, corporaciones u organizaciones que los adquieren a ECLIPSOFT (directamente o a través de un tercero) para su uso en su ámbito corporativo empresarial, corporativo u organizativo, y se encuentran identificados en los certificados.
- Las personas naturales que adquieren los certificados para sí mismas, y se encuentran identificados en los certificados.

El suscriptor del servicio de certificación adquiere una licencia de uso del certificado, para su uso propio o al objeto de facilitar la certificación de la identidad de una persona concreta debidamente autorizada para diversas actuaciones en el ámbito organizativo del suscriptor. En este último caso, esta persona figura identificada en el certificado.

El suscriptor del servicio electrónico de certificación es, por tanto, el cliente del prestador de servicios de certificación, de acuerdo con la legislación privada, y tiene los derechos y obligaciones que se definen por el prestador del servicio de certificación, que son adicionales y se entienden sin perjuicio de los derechos y obligaciones de los firmantes.

1.4.3.2. FIRMANTES

Los firmantes son las personas naturales que poseen de forma exclusiva las claves de firma electrónica para autenticación y/o firma electrónica; siendo típicamente los empleados, representantes legales o voluntarios, así como otras personas vinculadas a los suscriptores.

Los firmantes se encuentran debidamente autorizados por el suscriptor y debidamente identificados en el certificado mediante su nombre y apellidos, y número de identificación inequívoco, sin que sea posible, en general, el empleo de seudónimos.
La clave privada de un firmante no puede ser recuperada o deducida por la Entidad de Certificación de Información, por lo que las personas naturales identificadas en los correspondientes certificados son las únicas responsables de su protección y deberían considerar las implicaciones de perder una clave privada.

Dada la existencia de certificados para usos diferentes de la firma electrónica, como la autenticación, también se emplea el término más genérico de "persona natural identificada en el certificado", siempre con pleno respeto al cumplimiento de la regulación de firma electrónica en relación con los derechos y obligaciones del firmante.

1.4.3.3. PARTES USUARIAS

Las partes usuarias son las personas y las organizaciones que reciben firmas electrónicas y certificados digitales.
Como paso previo a confiar en los certificados, las partes usuarias deben verificarlos, como se establece en esta declaración de prácticas de certificación y en las correspondientes instrucciones disponibles en la página web de la Entidad de Certificación.

1.4.4. PROVEEDOR DE SERVICIOS DE INFRAESTRUCTURA DE CLAVE PÚBLICA

ECLIPSOFT y Uanataca, S.A. (en adelante UANATACA) han suscrito un contrato de prestación de servicios de tecnología en el que UANATACA proveerá la infraestructura de clave pública (PKI) que sustenta el servicio de certificación de ECLIPSOFT. Asimismo, UANATACA, pone a disposición de ECLIPSOFT, el personal técnico necesario para correcto desempeño de las funciones fiables propias de una Entidad de Certificación de Información.

Dicho lo cual, UANATACA se configura como el proveedor de servicios de Infraestructura para servicios de certificación, provee sus servicios tecnológicos a

ECLIPSOFT para que este pueda llevar a cabo los servicios inherentes a una Entidad de Certificación de Información, garantizando en todo momento la continuidad de los servicios en las condiciones y bajo los requisitos exigidos por la normativa.

Asimismo, se informa que UANATACA, es un Prestador de Servicios de Confianza acreditado conforme las previsiones del Reglamento Europeo No. 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).

La PKI de UANATACA se somete a auditorías anuales para la evaluación de la conformidad de prestadores cualificados de servicios de confianza de acuerdo con la normativa aplicable, bajo las normas:

- ISO/IEC 17065:2012
- ETSI EN 319 403
- ETSI EN 319 421
- ETSI EN 319 401
- ETSI EN 319 411-2
- ETSI EN 319 411-1

Asimismo, la PKI de UANATACA se somete a auditorías anuales bajo los estándares de calidad y seguridad:

- ISO 9001:2015
- ISO/IEC 27001:2022

1.4.4.1. OBLIGACIONES DEL PROVEEDOR DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA

El proveedor de la Infraestructura de Clave Pública se obliga a poner a disposición de ECLIPSOFT los servicios de tecnología necesarios para la prestación de servicios de certificación. En este sentido:

- El proveedor dispondrá del hardware necesario para que los mencionados servicios sean provistos con los niveles de seguridad requeridos por la normativa para tales fines.

- Dispondrá del software necesario para que los mencionados servicios sean provistos con los niveles de seguridad requeridos por la normativa para tales fines.
- Garantizará la custodia y hospedaje de los sistemas (hardware y software) en un Centro de Procesamiento de Datos (Data Center) con los niveles de seguridad lógica y física apropiados, de acuerdo con los estándares internacionales generalmente aceptados.
- Será responsable de realizar todos los mantenimientos preventivos, evolutivos, correctivos, reactivos y en general cualquier otro que requiera la infraestructura tecnológica para la prestación de los servicios de tecnología.
- Será responsable de la prestación de soporte técnico de 3er nivel, es decir, será responsable de prestar el soporte técnico en aquello que excede de la capacidad de gestión de ECLIPSOFT, y que está directamente vinculado a las deficiencias y/o fallos técnicos de la infraestructura tecnológica.

En la prestación de los servicios a ECLIPSOFT, el proveedor pondrá a disposición el personal técnico necesario para la operación de la infraestructura de clave pública, quienes ejercerán los roles fiables dedicados a la administración y operación de los sistemas, específicamente:

- Responsable de Seguridad PKI
- Auditor Interno
- Administrador de Sistemas
- Operador de Sistemas
- Administrador de CA

1.5. USO DE LOS CERTIFICADOS

Esta sección lista las aplicaciones para las que puede emplearse cada tipo de certificado, establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los certificados.

1.5.1. USOS PERMITIDOS PARA LOS CERTIFICADOS

Se deben tener en cuenta los usos permitidos indicados en los diversos campos de los perfiles de certificados, disponibles en el web https://firmas.eclipsoft.com

1.5.1.1. CERTIFICADO DE PERSONA NATURAL EN ARCHIVO

Este certificado dispone del **OID 1.3.6.1.4.1.57153.2.1.1**

Es un certificado de firma electrónica de acuerdo con lo establecido la Ley n.º. 2002-67 de comercio electrónico, firmas electrónicas y mensajes de datos, que se emite para la firma electrónica y autenticación.

Este certificado garantiza la identidad del firmante y su vinculación con el suscriptor (si lo hubiese) del servicio electrónico de certificación, y permite la generación de la "firma electrónica", es decir, la firma electrónica que está vinculada al firmante de manera única, permitiendo su identificación y ha sido generada utilizando medios que el firmante puede mantener bajo su control exclusivo, vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.

La firma electrónica generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 14 de la Ley nº. 2002-67 de comercio electrónico, firmas electrónicas y mensajes de datos.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital (Digital Signature, para realizar la función de autenticación)
b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c. Key Encipherment

1.5.1.2. CERTIFICADO DE PERSONA NATURAL EN DSCF

Este certificado dispone del **OID 1.3.6.1.4.1.57153.2.1.2**
Es un certificado de firma electrónica de acuerdo con lo establecido la Ley nº. 2002-67 de comercio electrónico, firmas electrónicas y mensajes de datos, que se emite para la firma electrónica y autenticación. El mismo se genera en un dispositivo seguro de creación de firma (DSCF).

Este certificado garantiza la identidad del firmante y su vinculación con el suscriptor (si lo hubiese) del servicio electrónico de certificación, y permite la generación de la "firma electrónica", es decir, la firma electrónica que está vinculada al firmante de manera única, permitiendo su identificación y ha sido generada utilizando medios que el firmante puede mantener bajo su control exclusivo, vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.
La firma electrónica generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 14 de la Ley nº. 2002-67 de comercio electrónico, firmas electrónicas y mensajes de datos.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a) Firma digital (Digital Signature, para realizar la función de autenticación)

b) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica

c) Key Encipherment

1.5.1.3. CERTIFICADO DE MIEMBRO DE EMPRESA O RELACIÓN DE DEPENDENCIA EN ARCHIVO

Este certificado dispone del **OID 1.3.6.1.4.1.57153.2.2.1**

Es un certificado de firma electrónica de acuerdo con lo establecido la Ley nº. 2002-67 de comercio electrónico, firmas electrónicas y mensajes de datos, que se emite para la firma electrónica y autenticación.

Este certificado garantiza la identidad del firmante y su vinculación con el suscriptor (si lo hubiese) del servicio electrónico de certificación, y permite la generación de la "firma electrónica", es decir, la firma electrónica que está vinculada al firmante de manera única, permitiendo su identificación y ha sido generada utilizando medios que el firmante puede mantener bajo su control exclusivo, vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.

La firma electrónica generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 14 de la Ley nº. 2002-67 de comercio electrónico, firmas electrónicas y mensajes de datos,

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital (Digital Signature, para realizar la función de autenticación)
b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c. Key Encipherment

1.5.1.4. CERTIFICADO DE MIEMBRO DE EMPRESA O EN RELACIÓN DE DEPENDENCIA EN DSCF

Este certificado dispone del **OID 1.3.6.1.4.1.57153.2.2.2**

Es un certificado de firma electrónica de acuerdo con lo establecido la Ley nº. 2002-67 de comercio electrónico, firmas electrónicas y mensajes de datos, que se emite para la firma electrónica y autenticación. El mismo se genera en un dispositivo seguro de creación de firma (DSCF).

Este certificado garantiza la identidad del firmante y su vinculación con el suscriptor (si lo hubiese) del servicio electrónico de certificación, y permite la generación de la "firma electrónica", es decir, la firma electrónica que está vinculada al firmante de manera única, permitiendo su identificación y ha sido generada utilizando medios que el firmante puede mantener bajo su control exclusivo, vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.

La firma electrónica generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 14 de la Ley nº. 2002-67 de comercio electrónico, firmas electrónicas y mensajes de datos.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.

b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital (Digital Signature, para realizar la función de autenticación)
b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c. Key Encipherment

1.5.1.5. CERTIFICADO DE REPRESENTANTE LEGAL EN ARCHIVO

Este certificado dispone del **OID 1.3.6.1.4.1.57153.2.3.1**
Es un certificado de firma electrónica de acuerdo con lo establecido la Ley nº. 2002-67 de comercio electrónico, firmas electrónicas y mensajes de datos, que se emite para la firma electrónica y autenticación.

El uso de este certificado garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y la entidad, empresa u organización descrita en el campo "O" (Organization), y permite la generación de la "firma electrónica", es decir, la firma electrónica que está vinculada al firmante de manera única, permitiendo su identificación y ha sido generada utilizando medios que el firmante puede mantener bajo su control exclusivo, vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.

La firma electrónica generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 14 de la Ley nº. 2002-67 de comercio electrónico, firmas electrónicas y mensajes de datos.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital (Digital Signature, para realizar la función de autenticación)
b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c. Key Encipherment

1.5.1.6. CERTIFICADO DE REPRESENTANTE LEGAL EN DSCF

Este certificado dispone del **OID 1.3.6.1.4.1.57153.2.3.2**

Es un certificado de firma electrónica de acuerdo con lo establecido la Ley nº. 2002-67 de comercio electrónico, firmas electrónicas y mensajes de datos, que se emite para la firma electrónica y autenticación. El mismo se genera en un dispositivo seguro de creación de firma (DSCF).

El uso de este certificado garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y la entidad, empresa u organización descrita en el campo "O" (Organization), y permite la generación de la "firma electrónica", es decir, la firma electrónica que está vinculada al firmante de manera única, permitiendo su identificación y ha sido generada utilizando medios que el firmante puede mantener bajo su control exclusivo, vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.

La firma electrónica generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en

relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 14 de la Ley nº. 2002-67 de comercio electrónico, firmas electrónicas y mensajes de datos.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital (Digital Signature, para realizar la función de autenticación)
b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c. Key Encipherment

1.5.1.7. CERTIFICADO DE SELLO ELECTRÓNICO EN ARCHIVO

Este certificado dispone del **OID 1.3.6.1.4.1.57153.102.2.4.1**

Es un certificado que se emite para la autenticación y la firma electrónica de una persona jurídica, de acuerdo con lo establecido la Ley nº. 2002-67 de comercio electrónico, firmas electrónicas y mensajes de datos, que se emite para la firma electrónica y autenticación.

Estos certificados garantizan la identidad de la entidad, empresa u organización suscriptora identificada en el certificado, y en su caso la del responsable de gestionar el certificado (si se hubiese identificado). Este certificado permite la generación de la "firma electrónica", es decir, la firma electrónica que está vinculada al firmante (entidad, empresa u organización) de manera única, permitiendo su identificación y ha sido generada utilizando medios que puede mantener bajo su control exclusivo,

vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.

La firma electrónica generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 14 de la Ley nº. 2002-67 de comercio electrónico, firmas electrónicas y mensajes de datos.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital (Digital Signature, para realizar la función de autenticación)
b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c. Key Encipherment

1.5.1.8. CERTIFICADO DE SELLO ELECTRÓNICO EN DSCF

Este certificado dispone del **OID 1.3.6.1.4.1.57153.102.2.4.2**

Es un certificado que se emite para la autenticación y la firma electrónica de una persona jurídica, de acuerdo con lo establecido la Ley nº. 2002-67 de comercio electrónico, firmas electrónicas y mensajes de datos, que se emite para la firma electrónica y autenticación. El mismo se genera en un dispositivo seguro de creación de firma.

Estos certificados garantizan la identidad de la entidad, empresa u organización suscriptora identificada en el certificado, y en su caso la del responsable de gestionar el certificado (si se hubiese identificado). Este certificado permite la generación de la "firma electrónica", es decir, la firma electrónica que está vinculada al firmante (entidad, empresa u organización) de manera única, permitiendo su identificación y ha sido generada utilizando medios que puede mantener bajo su control exclusivo, vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.

La firma electrónica generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 14 de la Ley nº. 2002-67 de comercio electrónico, firmas electrónicas y mensajes de datos.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital (Digital Signature, para realizar la función de autenticación)
b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c. Key Encipherment

1.5.1.9. CERTIFICADO DE SELLO DE TIEMPO ELECTRÓNICO

Este certificado dispone del **OID 1.3.6.1.4.1.57153.102.2.5.1**

Los certificados de sello de tiempo electrónico se tratan de certificados emitidos para la operación de autoridades de sellado de tiempo y hora, para la firma de los sellos de tiempo que éstas producen.

Estos certificados permiten la firma de los sellos de tiempo que se emiten, desde el momento que hayan obtenido un certificado de sello de tiempo electrónico válido y mientras éste se encuentre vigente.

La sincronización de los tiempos en ECLIPSOFT se realiza mediante un servicio servidor de tiempo NTP Stratum 3. Este servidor, un Meinberg Lantime M300/GPS, con oscilador TCXO de alta estabilidad, receptor GPS, formado por una tarjeta GPS interna para sincronizarse simultáneamente con los satélites con los que tiene visibilidad en cada momento (entre 3 y 8), y protección anti-rayos.

1.5.2. LÍMITES Y PROHIBICIONES DE USO DE LOS CERTIFICADOS

Los certificados se emplean para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.
Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la regulación aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Los certificados no pueden emplearse para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LRC).
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.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, de acuerdo esta Declaración de Prácticas de Certificación.

El empleo de los certificados digitales en operaciones que contravienen esta Declaración de Prácticas de Certificación, los documentos jurídicos vinculantes con cada certificado, o los contratos con las entidades de registro o con sus firmantes/suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a ECLIPSOFT, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

ECLIPSOFT no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de ECLIPSOFT emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado.

Asimismo, le será imputable al suscriptor, al firmante o a la persona responsable de la custodia, cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en esta Declaración de Prácticas de Certificación, los documentos jurídicos vinculantes con cada certificado, o los contratos o convenios con las entidades de registro o con sus suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

1.6. ADMINISTRACIÓN DE LA POLÍTICA

La administración, control de cambios, interpretación y gobierno de este documento, así como de las políticas de certificación y prácticas asociadas, es responsabilidad exclusiva ECLIPSOFT.

1.6.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Entidad: Eclipsoft S.A.

Dirección: Cdla. Kennedy Norte, Av. Miguel H. Alcivar Y Av. José Santiago Castillo. Edif. Blue Center, Piso 2 Oficina 1-6

Correo electrónico: info@eclipsoft.com

Página Web: www.firmas.eclipsoft.com

1.6.2. DATOS DE CONTACTO DE LA ORGANIZACIÓN ECLIPSOFT S.A.

Rol responsable 1:

Asegura la integridad y continuidad operativa de la infraestructura tecnológica que soporta los servicios de certificación, garantizando el cumplimiento de la DPC, los requisitos técnicos y de seguridad exigidos por la normativa ecuatoriana.

Nombres: Erik Ricardo Nevarez Benavidez - **Gerente de Tecnología**

Correo: enevarez@eclipsoft.com

Teléfono funcional: (593) 45001144

Disponibilidad: Lunes a viernes de 09:00 a 18:00, excluyendo días feriados oficiales.

Tiempo de respuesta: Un (1) día hábil, contado a partir de la recepción de la consulta.

Rol responsable 2: **Soporte de Certificación / Atención**

Gestionar las consultas e incidencias de los titulares de certificados digitales, orientándolos en los procesos de importación, renovación y uso correcto de sus firmas electrónicas, todo ello en estricto cumplimiento de lo establecido en la Declaración de Prácticas de Certificación (DPC).

Correo: firma.electronica@eclipsoft.com

Teléfono funcional: (593) 45001144 – (593) 998218016

Disponibilidad: Lunes a viernes de 09:00 a 18:00, excluyendo días feriados oficiales.

Tiempo de respuesta: Primera respuesta ≤ 8 horas hábiles.
(Revocación): en línea.

Rol responsable 3: **Mesa de ayuda y atención eventos críticos**

Brindar atención técnica y soporte continuo a los suscriptores de certificados electrónicos, realizando el diagnóstico preliminar de las incidencias reportadas en las plataformas donde interactúan nuestras firmas electrónicas (como servicios OCSP, CRL, repositorios de certificados y portales de gestión), asegurando una comunicación clara y oportuna sobre el estado operativo de dichas plataformas, y canalizando de manera restringida y supervisada los reportes de vulnerabilidades o eventos críticos que comprometan la seguridad de los certificados.

Correo: mesadeayuda@eclipsoft.com - operaciones@eclipsoft.com

Teléfono funcional: (593) 45001144 – (593) 983693136

Disponibilidad: 24/7

Tiempo de respuesta: Acuse de recepción en 2 horas máximo y actualización cada 4 horas máximo hasta el cierre definitivo del incidente.

1.6.3. PROCEDIMIENTOS DE GESTIÓN DEL DOCUMENTO

El sistema documental y de organización de ECLIPSOFT garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de este documento y de las especificaciones de servicio relacionados con el mismo.

2. PUBLICACIÓN DE INFORMACIÓN Y DEPÓSITO DE CERTIFICADOS

2.1. DEPÓSITO(S) DE CERTIFICADOS

ECLIPSOFT dispone de un Depósito de Certificados accesible de forma pública e ininterrumpida. Este repositorio es un servicio crítico para la confianza en el ecosistema del servicio de emisión de firmas electrónicas que proveemos.

- URL de Acceso: https://firmas.eclipsoft.com/
  - Certificados CA
  - CRL/LRC
  - OCSP
  - Certificados emitidos con consentimiento (cuando aplique)

ARQUITECTURA TÉCNICA Y ACUERDO DE NIVEL DE SERVICIO (SLA)

- **Infraestructura**: El Depósito de Certificados (Repositorio) de ECLIPSOFT opera sobre una infraestructura tecnológica de alta disponibilidad, diseñada con redundancia geográfica activa. Esto asegura la continuidad del servicio y la recuperación ante desastres, minimizando el impacto de fallos localizados.

- **Disponibilidad del Servicio:** ECLIPSOFT se compromete a mantener una disponibilidad media mensual del 99.5% para los servicios críticos. Este porcentaje se calcula sobre el total de minutos del mes, excluyendo períodos

de mantenimiento programado con notificación previa o causas de fuerza mayor.

- **Gestión de Incidencias:** Cuando se produzca indisponibilidad total o parcial del servicio, ECLIPSOFT se compromete a ejecutar acciones de recuperación automatizadas o manuales con el objetivo de restablecer la operatividad normal del servicio.

  El plazo máximo para dicha restauración será de 24 horas continuas (días calendario, incluyendo festivos y fines de semana), contadas a partir del momento de detección fehaciente del evento por parte de los sistemas de monitoreo de ECLIPSOFT.

  Cualquier ventana de mantenimiento que pudiera afectar el servicio será comunicada con al menos 24 horas de anticipación procurando minimizar el impacto en los usuarios.

2.2. PUBLICACIÓN DE INFORMACIÓN DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

ECLIPSOFT mantiene un Depósito de Certificados y Documentación Normativa de acceso público, libre y gratuito, accesible a través del URL operativa principal del repositorio: www.firmas.eclipsoft.com

Gestión de Certificados (LCM): https://lcm.modernpki.com/lcmpl
Consulta de certificados: https://consulta-firma.id4ec.com/

Este repositorio ha sido habilitado para garantizar la transparencia y el acceso a la información crítica que sustenta la validez jurídica de los certificados emitidos, en cumplimiento de la Ley de Comercio Electrónico y las resoluciones de ARCOTEL, donde mantenemos actualizada la siguiente información de carácter público:

Políticas y Prácticas aplicables:

- Declaración de Prácticas de Certificación (DPC) vigente y su historial de versiones

https://firmas.eclipsoft.com/dpc/

- Declaración de Prácticas de Certificación de Sellado de tiempo

https://firmas.eclipsoft.com/dpc_tsa/

- Modelo de contrato de prestación de servicio:

https://firmas.eclipsoft.com/contrato/

- Certificados de CA RAIZ y cadenas de certificación
- CRL vigentes y su historial
- Puntos de distribución (OSCP Y CRL)
- Tarifario público y condiciones de pago
- Datos de contacto

La publicación de CRL/OCSP se realiza de forma sincronizada entre todos los puntos de publicación redundantes, asegurando consistencia de la información.

Descarga de CRL´s y Servicio OCSP

ECLIPSOFT CA RAIZ (ARL´S)

http://crl1.modernpki.com/tsp/crl/arl_eclipsoft.crl

http://crl2.modernpki.com/tsp/crl/arl_eclipsoft.crl

ECLIPSOFT CA Subordinada 01 (CRL´S)

http://crl1.modernpki.com/tsp/crl/crl_eclipsoft.crl

http://crl2.modernpki.com/tsp/crl/crl_eclipsoft.crl

CA1 2016 RAIZ (ARL´S)

http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl

http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl

CA1 Subordinada 2016 (CRL´S)
http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl
http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl

Publicación de OCSP
ECLIPSOFT CA Subordinada 01
http://ocsp1.modernpki.com/tsp/ocsp/
http://ocsp2.modernpki.com/tsp/ocsp/

CA1 2016
http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/

ECLIPSOFT se reserva el derecho de modificar la estructura del portal corporativo, siempre garantizando la continuidad y el acceso público a la información aquí descrita mediante las redirecciones técnicas necesarias.

Información interna o de acceso restringido (no público)

Se considera información de acceso restringido toda aquella que, por su naturaleza crítica para la seguridad, la confidencialidad de los suscriptores o la operación confiable del servicio de certificación no es objeto de publicación. Su divulgación no autorizada podría comprometer la integridad, disponibilidad o el cumplimiento normativo de la Entidad de Certificación.

Esta categoría incluye, de manera enunciativa más no limitativa, lo siguiente:

- Expedientes de identificación y validación de suscriptores y titulares

Datos personales, documentos de identidad, y cualquier otro elemento probatorio recabado durante los procesos de registro y verificación.

Fundamento: Ley de Protección de datos personales y prevención de suplantación de identidad.

- Registros internos de auditoría, bitácoras operativas y evidencias de seguridad

Todos los logs de eventos de seguridad, trazabilidad de operaciones críticas, y registros de monitoreo no destinados a divulgación pública, excepto aquellos fragmentos que por mandato legal o regulatorio deban ser entregados a auditores o autoridades competentes.

- Procedimientos internos de seguridad y configuración sensible

Procedimientos internos de seguridad, hardening, configuraciones de sistemas, planes de continuidad de negocio, diagramas de arquitectura de red, inventario de activos críticos, y cualquier detalle que revele medidas de defensa en profundidad.

Fundamento: Evitar que un atacante pueda anticipar o neutralizar los controles de seguridad.

- Material criptográfico y datos de activación

Claves privadas (incluyendo claves de CA, claves de firma, de cifrado y de respaldo), parámetros de generación de claves, valores de activación (PIN, PUK, códigos OTP), y registros de ceremonias de generación de claves.

Fundamento: La confidencialidad del material criptográfico es esencial para el no repudio y la integridad de los certificados.

- Reportes de incidentes y vulnerabilidades con detalle técnico

Salvo obligación legal o regulatoria expresa de notificación

- Contratos y acuerdos con terceros y Entidades de Registro (ER)

Acuerdos de suscripción, contratos de servicio y acuerdos operativos con terceros proveedores de servicios de confianza. Solo será divulgado aquello estrictamente exigible por el marco normativo aplicable.

Fundamento: Protección de secretos comerciales, confidencialidad entre partes y cumplimiento de cláusulas de no divulgación.

2.3. FRECUENCIA DE PUBLICACIÓN

ECLIPSOFT establece los siguientes períodos y horarios para la publicación y actualización de la información como Entidad de Certificación, en cumplimiento de la normativa vigente y asegurando la transparencia y trazabilidad de los certificados emitidos:

a) Publicación de Información Normativa y Certificados Emitidos:

Declaración de Prácticas de Certificación (DPC): Se publica en el repositorio de Certificados de forma inmediata, una vez que se encuentran aprobada y vigente. Cualquier nueva versión reemplaza automáticamente a la anterior, manteniendo disponible el historial de versiones obligatoriamente.

Certificados de la Entidad de Certificación (Raíz y Subordinadas): Se publican de forma inmediata, posterior a su emisión o renovación, garantizando la disponibilidad de la cadena de confianza.

Certificados Emitidos a Suscriptores: La información sobre los certificados emitidos se refleja en los servicios de estado (CRL/OCSP) conforme a los plazos establecidos en los literales siguientes.

b) Publicación del Estado de Vigencia de Certificados (CRL - Listas de Revocación):

ECLIPSOFT genera y publica una LRC ordinaria al menos cada 24 horas, asegurando que exista siempre una versión vigente y actualizada de la lista de revocación.

Frecuencia ordinaria de emisión de LRC

Horarios programados de generación (UTC):

00:00 UTC (19:00 hora Ecuador, UTC-5)

12:00 UTC (07:00 hora Ecuador, UTC-5)

Actualización extraordinaria por evento de revocación, suspensión o reactivación

Cuando ocurra un evento que modifique el estado de un certificado (revocación, suspensión o reactivación), ECLIPSOFT generará y publicará una CRL extraordinaria en un plazo máximo de 2 horas desde la confirmación y registro del evento en el sistema de gestión del ciclo de vida del certificado.

Plazo de publicación de la CRL tras su generación

Toda CRL (tanto ordinaria como extraordinaria) se publica en el Depósito de ECLIPSOFT en un plazo no mayor a 2 horas desde su generación.

Consistencia entre puntos de publicación redundantes (CRL / OCSP)

ECLIPSOFT dispone de puntos de publicación redundantes para las CRL y para el servicio OCSP, según se define en el repositorio. La publicación se realiza de forma sincronizada entre todos estos puntos, garantizando que, en todo momento, la información de revocación sea idéntica y consistente independientemente del punto de publicación que consulte el cliente.

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de ECLIPSOFT, ésta deberá realizar sus mejores esfuerzos por asegurar que este servicio se mantenga inactivo el mínimo tiempo posible, que no podrá superar las 24 horas.

c) Actualizaciones Extraordinarias por Contingencia:

En caso de fallo técnico que impida la publicación en los horarios establecidos, ECLIPSOFT activará sus procedimientos de contingencia para restaurar el servicio y publicar la información pendiente en el menor tiempo posible, sin superar las 4 horas desde la detección del incidente, garantizando así la continuidad del servicio de validación.

Los terceros deben comprobar el estado de aquellos certificados un método por el cual se puede verificar el estado de los certificados es consultando la Lista de Revocación de Certificados más reciente emitida por la Entidad de Certificación de ECLIPSOFT.

Las Listas de Revocación de Certificados se publican en el Depósito de la Entidad de Certificación, así como en las siguientes direcciones web, indicadas dentro de los certificados:

- http://crl1.modernpki.com/tsp/crl/crl_eclipsoft.crl
- http://crl2.modernpki.com/tsp/crl/crl_eclipsoft.crl

El estado de la vigencia de los certificados también se puede comprobar por medio del protocolo OCSP.

- http://ocsp1.modernpki.com/tsp/ocsp/
- https://ocsp2.modernpki.com/tsp/ocsp/

Para garantizar la precisión en la gestión de revocación de certificados de la Autoridad de Certificación, los sistemas involucrados en la emisión y publicación de Listas de Revocación de Certificados (CRL) se sincronizan con UTC al menos una vez al día.
Las CRL se publican en el Depósito en un periodo inmediato razonable tras su generación, que en ningún caso supera unos pocos minutos.

2.4. CONTROL DE ACCESO

ECLIPSOFT garantiza el acceso de lectura público, libre y gratuito a la información del Depósito de Certificados descrita en la sección 2.2.
Con el objetivo de proteger la integridad, autenticidad y confidencialidad de la información, especialmente la relativa al estado de revocación de certificados (CRL/OCSP) y los certificados raíz de la jerarquía ha implementado sistemas fiables para la operación del Depósito, garantizando los siguientes principios de seguridad:

a) Mecanismos de Autenticación:
Autenticación Multifactor (MFA) obligatoria: Todo el personal debe autenticarse mediante MFA, para acceder a:

- Sistemas de gestión de certificados y de ciclo de vida.
- Repositorios de LRC y OCSP.
- Sistemas de emisión y firma de certificados.
- Bases de datos con información de suscriptores.

- Sistemas de auditoría y logs.
- Infraestructura de claves (HSM, generación de claves, ceremonias).
- Entornos de administración del Depósito y de la DPC.

Cada miembro del personal recibe una llave de seguridad personal e intransferible

Control de Acceso Basado en Roles (RBAC): El acceso está estrictamente establecido por perfiles de usuario con privilegios específicos. Se definen, al menos, los siguientes roles:

Administrador del Sistema: Responsable de la gestión técnica de la infraestructura (servidores, copias de seguridad, actualizaciones). No tiene permisos para modificar el contenido normativo (DPC, Políticas) ni las listas de certificados.

Operador de Autoridad de Registro (RAO): Personal autorizado para gestionar el ciclo de vida de los certificados (emisión, revocación, suspensión).

Calidad y cumplimiento Normativo: Responsable de publicar y actualizar la DPC, Políticas de Certificación y Acuerdos de Suscriptor. Sin acceso a la gestión criptográfica de certificados.

Auditor: Perfil de solo lectura que permite revisar logs y configuraciones sin capacidad de modificación.

Listas de Control de Acceso: Se implementan ACL a nivel de sistema operativo, base de datos y aplicación, restringiendo el acceso a los directorios y archivos del Depósito, únicamente a las cuentas de servicio y usuarios administrativos expresamente autorizados según su rol.

Periocidad: Al menos dos (2) veces por año (semestralmente), se realiza una revisión formal de todos los roles, permisos y listas de control de acceso (ACL) asociados a los sistemas críticos del Depósito y la infraestructura PKI.

Revisión de logs: Ante cualquier incidente y/o alerta generada por los sistemas de monitoreo de integridad

Auditoría interna: Al menos una (1) vez al año (anual) o cuando lo exija la normativa vigente.

b) Protección de la Integridad y Autenticidad de la Información:
Firmado criptográfico de CRL: Todas las Listas de Revocación de Certificados (CRL) publicadas están firmadas digitalmente por la Autoridad de Certificación correspondiente, permitiendo a cualquier usuario verificar su autenticidad e integridad mediante la clave pública del emisor.

Protección del certificado raíz y claves privadas:
El certificado raíz autofirmado (ECLIPSOFT CA ROOT) se mantiene almacenado en un módulo de seguridad hardware (HSM) con certificación FIPS 140-2 Nivel 3 o superior, fuera de línea y en una ubicación con doble control de acceso físico.

Mecanismos de integridad del sistema: Se emplean sumas de comprobación (hashes) y sistemas de detección de cambios (IDS) en los archivos críticos del Depósito para alertar sobre cualquier modificación no autorizada.

c) Registro y Trazabilidad (Pistas de Auditoría):
Registro de eventos (Logging): Se genera y conserva un registro detallado e inmutable de todas las acciones administrativas sobre el Depósito, incluyendo:

- Fecha y hora exacta
- Identidad del administrador (usuario y rol).
- Acción realizada
- Dirección IP origen.
- Resultado de la acción (éxito/fracaso).

Conservación de logs: Los registros de auditoría se almacenan de forma segura, con protección contra alteraciones, a disposición de ARCOTEL y auditorías externas.

d) Verificación Periódica y Compromisos de Auditoría:
Auditorías externas anuales: ECLIPSOFT se compromete a someter su infraestructura, a una auditoría de seguridad externa e independiente al menos una vez al año, realizada por una firma especializada en PKI y cumplimiento normativo.

Pruebas de penetración: Se realizarán pruebas de penetración (pentesting) periódicas sobre la infraestructura para identificar y corregir posibles vulnerabilidades que pudieran comprometer los controles de acceso por una entidad externa especializada de manera anual y cuando se presenten vulnerabilidades.

Detección de cambios técnicos: Se monitoriza continuamente la infraestructura para detectar cualquier cambio técnico (actualizaciones de software, parches de seguridad, modificaciones de configuración) que pueda afectar los requisitos de seguridad establecidos, siguiendo un proceso formal de gestión de cambios.

Resultados de auditorías: Los informes resumen de las auditorías externas (sin incluir información confidencial de seguridad) estarán a disposición de los suscriptores y partes usuarias que lo soliciten, como evidencia del compromiso de ECLIPSOFT con la transparencia y la mejora continua.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. REGISTRO INICIAL

3.1.1.TIPOS DE NOMBRES

Todos los certificados contienen un nombre distintivo (DN o distinguished name) conforme al estándar X.501 en el campo Subject, incluyendo un componente Common Name (CN=), relativo a la identidad del suscriptor y de la persona natural identificada

en el certificado, así como diversas informaciones de identidad adicionales en el campo SubjectAlternativeName.

Los nombres contenidos en los certificados son los siguientes:

3.1.1.1. CERTIFICADO DE PERSONA NATURAL EN ARCHIVO

Campo	Dato	Descripción
Country (C)	País	Código de país de dos letras, según ISO 3166-1 Por ejemplo: EC
Locality (L)	Ciudad	Nombre completo de la ciudad del domicilio
Title		Título o especialidad de firmante (opcional)
Surname	Apellidos del firmante	
Given Name	Nombres del firmante	
Serial Number	CI/CC/Pasaporte/ u otro	Número de identificación idóneo del firmante, reconocido en derecho
Organization Identifier	Número de RUC	Opcional
Common Name (CN)	Nombres y apellidos del firmante	

3.1.1.2. CERTIFICADO DE PERSONA NATURAL EN DSCF

Campo	Dato	Descripción
Country (C)	País	Código de país de dos letras, según ISO 3166-1 Por ejemplo: EC
Locality (L)	Ciudad	Nombre completo de la ciudad del domicilio
Title		Título o especialidad de firmante (opcional)
Surname	Apellidos del firmante	

Given Name	Nombres del firmante	
Serial Number	CI/CC/Pasaporte/ u otro	Número de identificación idóneo del firmante, reconocido en derecho
Organization Identifier	Número de RUC	Opcional
Common Name (CN)	Nombres y apellidos del firmante	

3.1.1.3. CERTIFICADO DE PERSONA NATURAL MIEMBRO DE EMPRESA O EN RELACIÓN DE DEPENDENCIA EN ARCHIVO

Campo	Dato	Descripción
Country (C)	País	Código de país de dos letras, según ISO 3166-1 Por ejemplo: EC
Locality (L)	Ciudad	Nombre completo de la ciudad del domicilio
Organization (O)		Organización a la que está vinculado el firmante
Organization Unit (OU)		Departamento o área de la Organización a la que está vinculado el firmante
Organization Identifier	Número de RUC	De la organización o Relación de Dependencia a la que está vinculado el firmante
Title	Título o especialidad de firmante	
Surname	Apellidos del firmante	
Given Name	Nombres del firmante	
Serial Number	CI/CC/Pasaporte/ u otro	Número de identificación idóneo del firmante, reconocido en derecho

Common Name (CN)	Nombre y apellidos del firmante	

3.1.1.4. CERTIFICADO DE PERSONA NATURAL MIEMBRO DE EMPRESA O EN RELACIÓN DE DEPENDENCIA EN DSCF

Campo	Dato	Descripción
Country (C)	País	Código de país de dos letras, según ISO 3166-1 Por ejemplo: EC
Locality (L)	Ciudad	Nombre completo de la ciudad del domicilio
Organization (O)		Organización a la que está vinculado el firmante
Organization Unit (OU)		Departamento o área de la Organización a la que está vinculado el firmante
Organization Identifier	Número de RUC	De la organización o Relación de Dependencia a la que está vinculado el firmante
Title	Título o especialidad de firmante	
Surname	Apellidos del firmante	
Given Name	Nombres del firmante	
Serial Number	CI/CC/Pasaporte/ u otro	Número de identificación idóneo del firmante, reconocido en derecho
Common Name (CN)	Nombres y apellidos del firmante	

3.1.1.5. CERTIFICADO DE REPRESENTANTE LEGAL EN ARCHIVO

Campo	Dato	Descripción
Country (C)	País	Código de país de dos letras, según ISO 3166-1 Por ejemplo: EC
Locality (L)	Ciudad	Nombre completo de la ciudad del domicilio
Organization (O)		Organización que representa el firmante
Organization Unit (OU)		Unidad de la Organización a la que está vinculado el firmante
Organization Identifier	Número de RUC	De la organización a la que está vinculado el firmante
Title	Tipo de representación	
Surname	Apellidos del firmante	
Given Name	Nombres del firmante	
Serial Number	CI/CC/Pasaporte/ u otro	Número de identificación idóneo del firmante reconocido en derecho
Common Name (CN)	Nombres y apellidos del representante	

3.1.1.6. CERTIFICADO DE REPRESENTANTE LEGAL EN DSCF

Campo	Dato	Descripción
Country (C)	País	Código de país de dos letras, según ISO 3166-1 Por ejemplo: EC
Locality (L)	Ciudad	Nombre completo de la ciudad del domicilio
Organization (O)		Organización que representa el firmante

Organization Unit (OU)		Unidad de la Organización a la que está vinculado el firmante
Organization Identifier	Número de RUC	De la organización a la que está vinculado el firmante
Title	Tipo de representación	
Surname	Apellidos del firmante	
Given Name	Nombres del firmante	
Serial Number	CI/CC/Pasaporte/ u otro	Número de identificación idóneo del firmante reconocido en derecho
Common Name (CN)	Nombres y apellidos del representante	

3.1.1.7. CERTIFICADO DE SELLO ELECTRÓNICO EN ARCHIVO

Campo	Dato	Descripción
Country (C)	País	Código de país de dos letras, según ISO 3166-1 Por ejemplo: EC
Organization (O)		Nombre de la Organización
Organization Unit (OU)		Nombre de la Unidad
Organization Identifier	RUC	Número de identificación fiscal de la Organización precedido del texto VATEC-
Serial Number	RUC	De la Entidad
Common Name (CN)		Denominación de sistema o aplicación de proceso automático

3.1.1.8. CERTIFICADO DE SELLO ELECTRÓNICO EN DSCF

Campo	Dato	Descripción
Country (C)	País	Código de país de dos letras, según ISO 3166-1 Por ejemplo: EC
Organization (O)		Nombre de la Organización
Locality (L)	Ciudad	Nombre completo de la ciudad del domicilio
Organization Unit (OU)		Nombre de la Unidad
Organization Identifier	RUC	Número de identificación fiscal de la Organización precedido del texto VATEC-
Serial Number	RUC	De la Entidad
Common Name (CN)		Denominación de sistema o aplicación de proceso automático

3.1.1.9. CERTIFICADO DE SELLO CUALIFICADO DE TIEMPO ELECTRÓNICO

Campo	Dato	Descripción
Country (C)	País	Código de país de dos letras, según ISO 3166-1 Por ejemplo: EC
Organization (O)		Nombre de la Organización
Locality (L)	Ciudad	Nombre completo de la ciudad del domicilio
Organization Identifier	RUC	Número de identificación fiscal de la Organización precedido del texto VATEC-
Serial Number	RUC	De la Entidad

Common Name (CN)		Nombre del servicio
Organizational Unit (OU)		Unidad que presta el servicio

3.1.2.SIGNIFICADO DE LOS NOMBRES

Los nombres contenidos en los campos SubjectName y SubjectAlternativeName de los certificados son comprensibles en lenguaje natural, de acuerdo con lo establecido en la sección anterior.

3.1.2.1. EMISIÓN DE CERTIFICADOS DEL SET DE PRUEBAS Y CERTIFICADOS DE PRUEBAS EN GENERAL

Queda estrictamente prohibida la emisión certificados de firma electrónica con fines de prueba, evaluación, validación o desarrollo que haga uso de la jerarquía de certificación, los sistemas, las políticas de certificación o los recursos de infraestructura de clave pública (PKI) de ECLIPSOFT.

Entorno de pruebas aislado e independiente

Toda actividad de prueba interna, incluyendo, pero no limitándose a pruebas funcionales, de integración, rendimiento o aceptación, deberá ejecutarse exclusivamente en un entorno de laboratorio aislado. Dicho entorno deberá contar con una PKI de pruebas propia, completamente independiente, que utilice su propia jerarquía raíz y políticas de certificación diferenciadas sin vinculación técnica ni de confianza con los certificados raíz de producción de ECLIPSOFT.

3.1.3.EMPLEO DE ANÓNIMOS Y SEUDÓNIMOS

En ningún caso se pueden utilizar seudónimos para identificar una entidad, empresa u organización, ni a un firmante. Así mismo, en ningún caso se emiten certificados anónimos.

3.1.4.INTERPRETACIÓN DE FORMATOS DE NOMBRES

Los formatos de nombres se interpretarán de acuerdo con la ley del país de establecimiento del suscriptor, en sus propios términos.

El campo "país" o "estado" será el del suscriptor del certificado.

Los certificados cuyos suscriptores sean personas jurídicas, entidades u organismos de la administración pública, muestran la relación entre estas y una persona natural, con independencia de la nacionalidad de la persona natural.

En el campo "número de serie" se incluye el número de Cédula, Pasaporte u otro número de identificación idóneo del firmante, reconocido en derecho.

3.1.5.UNICIDAD DE LOS NOMBRES

Los nombres de los suscriptores de certificados serán únicos, para cada política de certificado de ECLIPSOFT.

No se podrá asignar un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente, situación que, en principio no se ha de dar, gracias a la presencia del número del Número de Identificación Fiscal, o equivalente, en el esquema de nombres.

Un suscriptor puede pedir más de un certificado siempre que la combinación de los siguientes valores existentes en la solicitud fuera diferente de un certificado válido:

- Número de Identificación Fiscal (RUC) u otro identificador legalmente válido de la persona natural.
- Número de identificación u otro identificador legalmente válido del suscriptor.
- Tipo de certificado (OID de identificador de política de certificación).
- Soporte del certificado (software o en dispositivo seguro de creación de firma)

Como excepción esta DPC permite emitir un certificado cuando coincida RUC del suscriptor, RUC o documento de identidad del firmante, Tipo de certificado, Soporte del certificado, con un certificado activo, siempre que exista algún elemento diferenciador entre ambos, en los campos cargo (title) y/o departamento (Organizational Unit).

3.1.6.RESOLUCIÓN DE CONFLICTOS RELATIVOS A NOMBRES

Los solicitantes de certificados no incluirán nombres en las solicitudes que puedan suponer infracción, por el futuro suscriptor, de derechos de terceros.

ECLIPSOFT no estará obligada a determinar previamente que un solicitante de certificados tiene derechos de propiedad industrial sobre el nombre que aparece en una solicitud de certificado, sino que en principio procederá a certificarlo.

Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

Sin embargo, en caso de recibir una notificación relativa a un conflicto de nombres, conforme a la legislación del país del suscriptor, podrá emprender las acciones pertinentes orientadas a bloquear o retirar el certificado emitido.

En todo caso, la Entidad de Certificación de Información se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

Toda controversia o conflicto que se derive del presente documento se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro, en el marco de la entidad de Arbitraje que corresponda a la República del Ecuador, de conformidad con sus normas y disposiciones, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte en el documento contractual que formaliza el servicio.

3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD

La identidad de los suscriptores de certificados resulta fijada en el momento de la firma del contrato entre ECLIPSOFT y el suscriptor, previa verificación de la existencia del suscriptor a través de los procedimientos de reconocimiento establecidos y mediante la comprobación de su documento oficial de identidad o las escrituras correspondientes, al igual que los poderes de actuación de la persona que presente como representante si fuese el caso. Para esta verificación, se podrá emplear documentación pública o notarial, o la consulta directa a los registros públicos correspondientes.

En el caso de personas naturales identificadas en certificados cuyo suscriptor sea una persona jurídica, sus identidades se validarán mediante los registros corporativos de

la entidad, empresa u organización de derecho público o privado, suscriptoras de los certificados. El suscriptor producirá una certificación de los datos necesarios, y la remitirá a ECLIPSOFT, por los medios que ésta habilite, para el registro de la identidad de los firmantes.

3.2.1. PRUEBA DE POSESIÓN DE CLAVE PRIVADA

La posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del certificado por el suscriptor, en certificados de sello, o por el firmante, en certificados de firma.

3.2.2. AUTENTICACIÓN DE LA IDENTIDAD DE UNA ORGANIZACIÓN, EMPRESA O ENTIDAD MEDIANTE REPRESENTANTE

Las personas naturales con capacidad de actuar en nombre de las personas jurídicas o entidades sin personalidad jurídica, públicas o privadas, que sean suscriptoras de certificados, podrán actuar como representantes de estas, siempre y cuando exista una situación previa de representación legal o voluntaria entre la persona natural y la organización de la que se trate, que exige su reconocimiento por ECLIPSOFT, la cual se realizará mediante el siguiente procedimiento:

1. El representante del suscriptor deberá acreditar su identidad por uno de los siguientes métodos:
    - (i) Identificándose presencialmente ante un operador o persona autorizada de una Entidad de Registro de ECLIPSOFT:
        - Mostrando su Documento de Identidad, pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.
        - Acreditando el carácter y facultades que alegue poseer.

    - (ii) Identificándose electrónicamente a través del sistema de video identificación remota de ECLIPSOFT:
        - Mostrando su Documento de Identidad, pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.

- Proveyendo prueba de vida mediante el uso de medios técnicos de captación de imágenes y vídeo utilizando algoritmos de criptografía biométrica facial e inteligencia artificial para el cotejo inequívoco de la identidad del solicitante y la verificación de la prueba de vida de éste, así como de la autenticidad del documento de identidad exhibido.
- Acreditando el carácter y facultades que alegue poseer.

2. El representante proporcionará la siguiente información y sus correspondientes soportes acreditativos:
    - Sus datos de identificación, como representante:
        - Nombre y apellidos
        - Documento: Documento de Identidad, pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.
    - Los datos de identificación del suscriptor al que representa:
        - Denominación o razón social.
        - Toda información de registro existente, incluyendo los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante.
        - Documento: RUC o documento acreditativo de la identificación fiscal de la entidad.
        - Documento: Documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, 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.
    - Los datos relativos a la representación o la capacidad de actuación que ostenta:
        - La vigencia de la representación o la capacidad de actuación (fecha de inicio y fin) si resulta aplicable.

- El ámbito y los límites, en su caso, de la representación o de la capacidad de actuación:
  - TOTAL. Representación o capacidad total. Esta comprobación se podrá realizar mediante consulta telemática al registro público donde conste inscrita la representación.
  - PARCIAL. Representación o capacidad parcial. Esta comprobación se podrá realizar mediante copia auténtica electrónica de la escritura notarial de apoderamiento, en los términos de la normativa notarial.

3. El operador o personal autorizado de la Entidad de Registro de ECLIPSOFT comprobará la identidad del representante actuando del siguiente modo:
   - Cuando la identificación se haya realizado presencialmente, a través de la revisión de:
     - Documento de identidad aportado.
     - Documentación que acredite su representación.
   - Cuando la identificación se haya realizado a través del método de identificación electrónica a través de video identificación de ECLIPSOFT mediante:
     - Revisión de los vídeos e imágenes captadas del documento de identificación aportado y del propio solicitante.
     - Revisión de la prueba de vida del solicitante, a través de los resultados facilitados por el sistema de video identificación remota.
     - Revisión del cotejo producido por el sistema de video identificación remota de la fotografía del documento de identidad con las imágenes y vídeo obtenido durante el registro del solicitante.
     - Revisión producida por el sistema de video identificación remota, a través de inteligencia artificial para la detección de documentos de identidad falsos.
     - Documentación que acredite su representación.

4. Alternativamente, se podrá legitimar notarialmente la firma del formulario, y hacerse llegar al operador o personal autorizado de la Entidad de Registro ECLIPSOFT por correo postal certificado, en cuyo caso el paso anterior no será preciso.

La prestación del servicio de certificación digital se formaliza mediante el oportuno contrato entre ECLIPSOFT y el suscriptor, debidamente representado.

3.2.3.AUTENTICACIÓN DE LA IDENTIDAD DE UNA PERSONA NATURAL

Esta sección describe los métodos de comprobación de la identidad de una persona natural identificada en un certificado.

3.2.3.1. EN LOS CERTIFICADOS

La identidad de las personas naturales firmantes identificados en los certificados, se valida a través de uno de los siguientes métodos:

- (i) Identificándose presencialmente ante un operador o persona autorizada de una Entidad de Registro de ECLIPSOFT:
  - Mostrando su Documento de Identidad, pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.

- (ii) Identificándose electrónicamente a través del sistema de video identificación remota de ECLIPSOFT:
  - Mostrando su Documento de Identidad, pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.
  - Proveyendo prueba de vida mediante el uso de medios técnicos de captación de imágenes y vídeo utilizando algoritmos de criptografía biométrica facial e inteligencia artificial para el cotejo inequívoco de la identidad del solicitante y la verificación de la prueba de vida de éste, así como de la autenticidad del documento de identidad exhibido.

La información de identificación de las personas naturales identificadas en los certificados (i) cuyo suscriptor sea una entidad con o sin personalidad jurídica o (ii) ya constase la misma en virtud de una relación previa, la información podrá ser validada comparando la información de la solicitud con los registros de la entidad, empresa u organización de derecho público o privado a la que está vinculado, o bien con la documentación que esta haya suministrado sobre la persona natural que identifica como firmante, asegurando la corrección de la información a certificar.

3.2.3.2. VALIDACIÓN DE LA IDENTIDAD

El operador o personal autorizado de la Entidad de Registro de ECLIPSOFT comprobará la identidad de la persona natural identificada en la solicitud del certificado, actuando del siguiente modo:

- Cuando la identificación se haya realizado presencialmente, a través de la revisión de:
  - Documento de identidad aportado.

- Cuando la identificación se haya realizado a través del método de identificación electrónica a través de video identificación de ECLIPSOFT mediante:
  - Revisión de los vídeos e imágenes captadas del documento de identificación aportado y del propio solicitante.
  - Revisión de la prueba de vida del solicitante, a través de los resultados facilitados por el sistema de video identificación remota.
  - Revisión del cotejo producido por el sistema de video identificación remota de la fotografía del documento de identidad con las imágenes y vídeo obtenido durante el registro del solicitante.
  - Revisión producida por el sistema de video identificación remota, a través de inteligencia artificial para la detección de documentos de identidad falsos.

Para la solicitud de los certificados cuyo suscriptor sea una persona jurídica no se requiere identificación expresa, debido a la relación ya acreditada entre la persona natural y entidad, empresa u organización de derecho público o privado a la que está vinculada. Sin embargo, antes de la entrega de un certificado, la entidad, empresa u organización de derecho público o privado suscriptora, por medio de su responsable

de certificación, de tenerlo, u otro miembro designado, deberá contrastar la identidad de la persona natural identificada en el certificado mediante su presencia física o siguiendo el procedimiento de video identificación remota establecido por ECLIPSOFT.

Durante este trámite se confirma rigurosamente la identidad de la persona natural identificada en el certificado. Por este motivo, en todos los casos en que se expide un certificado se acredita a través de un operador de registro la identidad de la persona natural firmante, la Entidad de Registro verificará mediante la exhibición de documentos o a través de sus propias fuentes de información, el resto de los datos y atributos a incluir en el certificado, guardando documentación acreditativa de la validez de estos.

3.2.3.3. VINCULACIÓN DE LA PERSONA NATURAL

La justificación documental de la vinculación de una persona natural identificada en un certificado con la entidad, empresa u organización de derecho público o privado viene dada por su constancia en los registros internos (contrato de trabajo como empleado, o el contrato mercantil que lo vincula, o el acta donde se indique su cargo, o la solicitud como miembro de la organización…) de cada una de las personas públicas y privadas a las que están vinculadas.

3.2.4.INFORMACIÓN DE SUSCRIPTOR NO VERIFICADA

ECLIPSOFT no incluye ninguna información de suscriptor no verificada en los certificados.

3.2.5.AUTENTICACIÓN DE LA IDENTIDAD DE UNA ER Y SUS OPERADORES

Para la constitución de una nueva Entidad de Registro, ECLIPSOFT realiza las verificaciones necesarias para confirmar la existencia de la entidad u organización de la que se trate. Para ello, ECLIPSOFT podrá utilizar exhibición de documentos o utilizar sus propias fuentes de información.

Igualmente, ECLIPSOFT directamente o a través de su Entidad de Registro, verifica y valida la identidad de los operadores de las Entidades de Registro, para lo cual estas

últimas envían a ECLIPSOFT la documentación de identificación correspondientes al nuevo operador, juntamente con su autorización para actuar como tal.
En el caso de que el operador desee emitirse un certificado de cualquier otro tipo de perfil de certificado, siempre que cumpla las condiciones para poderse emitir, no podrá actuar como operador de registro para la solicitud de dicho certificado, debiendo ser dicho operador de registro una persona distinta a la solicitante del certificado.

ECLIPSOFT se asegura que los operadores de la Entidad de Registro reciben la formación suficiente para el desarrollo de sus funciones, lo cual verifica con la evaluación correspondiente. Dicha formación y evaluación puede ser ejecutada por la Entidad de Registro previamente autorizada por ECLIPSOFT.
Para la prestación de los servicios, ECLIPSOFT se asegura de que los operadores de Entidad de Registro acceden al sistema mediante autenticación fuerte.

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITUDES DE RENOVACIÓN

3.3.1. VALIDACIÓN PARA LA RENOVACIÓN RUTINARIA DE CERTIFICADOS

Antes de renovar un certificado, el operador o personal autorizado de la Entidad de Registro ECLIPSOFT comprueba que la información empleada para verificar la identidad y los restantes datos del suscriptor y de la persona natural identificada en el certificado continúan siendo válidos.
Los métodos aceptables para dicha comprobación son:

- El uso del código "CRE" o "ERC" relativo al certificado anterior, o de otros métodos de autenticación personal, que consiste en información que sólo conoce la persona natural identificada en el certificado, y que le permite renovar de forma automática su certificado, siempre que no se haya superado el plazo máximo legalmente establecido.
- El empleo del certificado vigente para su renovación y no se haya superado el plazo máximo legalmente establecido para esta posibilidad.

Si cualquier información del suscriptor o de la persona natural identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una identificación completa, de acuerdo con lo establecido en la sección 3.2.

3.3.2. IDENTIFICACIÓN Y AUTENTICACIÓN DE LA SOLICITUD DE RENOVACIÓN

Antes de renovar un certificado, el operador o personal autorizado de la Entidad de Registro ECLIPSOFT comprobará que la información empleada en su día para verificar la identidad y los restantes datos del suscriptor y de la persona natural identificada en el certificado continúa siendo válida, en cuyo caso se aplicará lo dispuesto en la sección anterior.

La renovación de certificados tras la revocación no será posible en los siguientes casos:

- El certificado fue revocado por emisión errónea a una persona diferente a la identificada en el certificado.
- El certificado fue revocado por emisión no autorizada por la persona natural identificada en el certificado.
- El certificado revocado puede contener información errónea o falsa.

Si cualquier información del suscriptor o de la persona natural identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una identificación completa, de acuerdo con lo establecido en la sección 3.2.

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN DE LA SOLICITUD DE REVOCACIÓN, SUSPENSIÓN O REACTIVACIÓN

ECLIPSOFT o un operador o personal autorizado de la Entidad de Registro autentica las peticiones e informes relativos a la revocación, suspensión o reactivación de un certificado, comprobando que provienen de una persona autorizada.

La identificación de los suscriptores y/o firmantes en el proceso de revocación, suspensión o reactivación de certificados podrá ser realizada por:

- El suscriptor y/o firmante:
    - Identificándose y autenticándose mediante el uso del Código de Revocación (ERC o ERC) a través de la página web de ECLIPSOFT en horario 24x7.

- Otros medios de comunicación, como el teléfono, correo electrónico, etc. cuando existan garantías razonables de la identidad del solicitante de la suspensión o revocación, a juicio de ECLIPSOFT y/o Entidades de Registro.

- Las Entidades de registro de ECLIPSOFT: deberán identificar al firmante ante una petición de revocación, suspensión o reactivación según los propios medios que considere necesarios.

Cuando en horario de oficina el suscriptor desee iniciar una petición de revocación y existan dudas para su identificación, su certificado pasa a estado de suspensión.

4. REQUISITOS DE OPERACIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS

4.1. SOLICITUD DE EMISIÓN DE CERTIFICADO

4.1.1.LEGITIMACIÓN PARA SOLICITAR LA EMISIÓN

El solicitante del certificado sea persona natural o jurídica debe firmar un contrato de prestación de servicios de certificación con ECLIPSOFT.

Asimismo, con anterioridad a la emisión y entrega de un certificado, debe existir una solicitud de certificados ya sea en el mismo contrato, en un documento específico de hoja de solicitud de certificados o ante la Entidad de Registro.

Cuando el solicitante es una persona distinta al suscriptor, debe existir una autorización del suscriptor para que el solicitante pueda realizar la solicitud, que se instrumenta jurídicamente mediante una hoja de solicitud de certificados suscrita por dicho solicitante en nombre propio en el caso de certificados para persona natural, o bien en nombre del suscriptor en el caso de que el suscriptor sea la por entidad, empresa u organización de derecho público o privado.

4.1.2.PROCEDIMIENTO DE ALTA Y RESPONSABILIDADES

ECLIPSOFT recibe solicitudes de certificados, realizadas por personas, entidades, empresas u organizaciones de derecho público o privado.

Las solicitudes se instrumentan mediante un formulario en formato papel o electrónico, de manera individual o por lotes, o mediante la conexión con bases de

datos externas, o a través de una capa de Web Services cuyo destinatario es ECLIPSOFT. En el caso de certificados cuyo suscriptor sea una entidad, empresa u organización de derecho público o privado que actúe como una Entidad de Registro de ECLIPSOFT, podrá gestionar directamente las solicitudes accediendo a los sistemas informáticos de ECLIPSOFT y generar los certificados correspondientes para la propia entidad, empresa u organización o para sus miembros.

A la solicitud se deberá acompañar documentación justificativa de la identidad y otras circunstancias de la persona natural identificada en el certificado, de acuerdo con lo establecido en la sección 3.2.3. También se deberá acompañar una dirección física, u otros datos, que permitan contactar a la persona natural identificada en el certificado.

4.2. PROCESAMIENTO DE LA SOLICITUD DE CERTIFICACIÓN

4.2.1. EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Una vez recibida una petición de certificado, ECLIPSOFT se asegura de que las solicitudes de certificado sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

En caso afirmativo, ECLIPSOFT verifica la información proporcionada, verificando los aspectos descritos en la sección 3.2

La documentación justificativa de la aprobación de la solicitud de un certificado debe ser conservada y debidamente registrada y con garantías de seguridad e integridad durante el plazo de 15 años desde la expiración del certificado, incluso en caso de pérdida anticipada de vigencia por revocación.

4.2.2. APROBACIÓN O RECHAZO DE LA SOLICITUD

En caso de que los datos se verifiquen correctamente, ECLIPSOFT debe aprobar la solicitud del certificado y proceder a su emisión y entrega.

Si la verificación indica que la información no es correcta, o si se sospecha que no es correcta o que puede afectar a la reputación de la Entidad de Certificación de Información, de las Entidades de Registro o de los suscriptores, ECLIPSOFT denegará la petición, o detendrá su aprobación hasta haber realizado las comprobaciones complementarias que considere oportunas.

En caso de que de las comprobaciones adicionales no se desprenda la corrección de las informaciones a verificar, ECLIPSOFT denegará la solicitud definitivamente.
ECLIPSOFT notifica al solicitante la aprobación o denegación de la solicitud.
ECLIPSOFT podrá automatizar los procedimientos de verificación de la corrección de la información que será contenida en los certificados, y de aprobación de las solicitudes.

4.2.3. PLAZO PARA RESOLVER LA SOLICITUD

ECLIPSOFT atiende las solicitudes de certificados por orden de llegada, en un plazo razonable, pudiendo especificarse una garantía de plazo máximo en el contrato de emisión de certificados.
Las solicitudes se mantienen activas hasta su aprobación o rechazo.

4.3. EMISIÓN DEL CERTIFICADO

4.3.1. ACCIONES DE LA CA DURANTE EL PROCESO DE EMISIÓN

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se pone a disposición del firmante para su aceptación.
Los procedimientos establecidos en esta sección también se aplican en caso de renovación de certificados, dado que la misma implica la emisión de un nuevo certificado.

Durante el proceso, ECLIPSOFT:

- Protege la confidencialidad e integridad de los datos de registro de que dispone.
- Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.

- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
- Indica la fecha y la hora en que se expidió un certificado.
- Garantiza el control exclusivo de las claves por parte del usuario, no pudiendo la propia ECLIPSOFT o sus Entidades de Registro deducirlas o utilizarlas en ningún modo.

4.3.2. NOTIFICACIÓN DE LA EMISIÓN AL SUSCRIPTOR

ECLIPSOFT notifica la emisión del certificado al suscriptor y/o a la persona natural identificada en el certificado y el método de generación/descarga.

4.4. ENTREGA Y ACEPTACIÓN DEL CERTIFICADO

4.4.1. RESPONSABILIDADES DE LA CA

Durante este proceso, el operador o personal autorizado de la Entidad de Registro ECLIPSOFT debe realizar las siguientes actuaciones:

- Acreditar definitivamente la identidad de la persona natural identificada en el certificado, de acuerdo con lo establecido en las secciones 3.2.2 y 3.2.3.
- Disponer del Contrato de Prestación de Servicios de Certificación debidamente firmado por el Suscriptor.
- Entregar la hoja de entrega y aceptación del certificado a la persona natural identificada en el certificado con los siguientes contenidos mínimos:
    - Información básica acerca del uso del certificado, incluyendo especialmente información acerca del prestador de servicios de certificación y de la Declaración de Prácticas de Certificación aplicable, como sus obligaciones, facultades y responsabilidades.
    - Información acerca del certificado.

- Reconocimiento, por parte del firmante, de recibir el certificado y/o los mecanismos para su generación/descarga y la aceptación de los citados elementos.
- Régimen de obligaciones del firmante.
- Responsabilidad del firmante.
- Método de imputación exclusiva al firmante, de su clave privada y de sus datos de activación del certificado, de acuerdo con lo establecido en las secciones 6.2 y 6.4.
- La fecha del acto de entrega y aceptación.

Toda esta información podrá incluirse en el propio Contrato de Prestación de Servicios de Certificación. Dicho lo cual, cuando se produzca la firma del Contrato Prestación de Servicios de Certificación por el Suscriptor, se entenderá perfeccionada la entrega y aceptación del certificado.

- Obtener la firma de la persona identificada en el certificado.

Las Entidades de Registro son las encargadas de realizar estos procesos, debiendo registrar documentalmente los anteriores actos y conserva los citados documentos originales (hojas de entrega y aceptación), remitiendo copia electrónica a ECLIPSOFT, así como los originales cuando ECLIPSOFT precise de acceso a los mismos.

4.4.2.CONDUCTA QUE CONSTITUYE ACEPTACIÓN DEL CERTIFICADO

Cuando se haga entrega de la hoja de aceptación, la aceptación del certificado por la persona natural identificada en el certificado se produce mediante la firma de la hoja de entrega y aceptación.

Cuando la generación y entrega del certificado se lleve a cabo a través del procedimiento automatizado definido por ECLIPSOFT, la aceptación del certificado por la persona natural identificada en el mismo se produce mediante la firma del contrato de Prestación de Servicios de Certificación utilizando el propio certificado.

4.4.3.PUBLICACIÓN DEL CERTIFICADO

ECLIPSOFT publica el certificado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes y siempre que ECLIPSOFT disponga de la autorización de la persona natural identificada en el certificado.

4.4.4.NOTIFICACIÓN DE LA EMISIÓN A TERCEROS

ECLIPSOFT no realiza ninguna notificación de la emisión a terceras entidades.

4.5. USO DEL PAR DE CLAVES Y DEL CERTIFICADO

Para garantizar la solidez y seguridad de los procesos criptográficos, ECLIPSOFT se adhiere a los siguientes estándares técnicos:

- **Generación de Claves:**
  - Claves de la Entidad de Certificación (AC Raíz y Subordinadas): Generadas y custodiadas exclusivamente en Módulos de Seguridad Hardware (HSM) con certificación FIPS 140-2 Nivel 3 (o superior).
  - Claves de Certificados en Archivo: Generadas por el software del solicitante, asegurando que la clave privada nunca sea exportada o conocida por la Entidad de Certificación.
  - Claves de Certificados en DSCF: Generadas y almacenadas dentro del perímetro de seguridad del propio Dispositivo Seguro de Creación de Firma (HSM).
- **Algoritmos y Tamaños de Clave:**
  - AC Raíz (ECLIPSOFT CA ROOT): RSA de 4096 bits con función hash SHA-384.
  - AC Subordinada (ECLIPSOFT CA1): RSA de 4096 bits con función hash SHA-256.
  - Certificados de Entidad Final (Todos los tipos): RSA de 2048 bits (como mínimo) con función hash SHA-256.
  - Algoritmos de Firma: El algoritmo de firma para todos los certificados emitidos bajo esta DPC será sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11), garantizando la interoperabilidad y un nivel de seguridad adecuado.

4.5.1.USO POR EL FIRMANTE

ECLIPSOFT obliga a:

- Facilitar a ECLIPSOFT información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en este documento.
- Reconocer su capacidad de producción de firmas electrónicas; esto es, equivalentes a firmas manuscritas.
- Ser especialmente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 6.1 y 6.2.
- Comunicar a ECLIPSOFT, Entidades de Registro y a cualquier persona que se crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
- Dejar de emplear la clave privada transcurrido el periodo indicado en la sección 6.3.2.

ECLIPSOFT obliga al firmante a responsabilizarse de:

- Que todas las informaciones suministradas por el firmante que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el firmante es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave

pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

4.5.2. USO POR EL SUBSCRIPTOR

4.5.2.1. OBLIGACIONES DEL SUSCRIPTOR DEL CERTIFICADO

ECLIPSOFT obliga contractualmente al suscriptor a:

- Facilitar a la Entidad de Certificación información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo estipulado en este documento.
- Comunicar a ECLIPSOFT, Entidades de Registro y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
    - La pérdida, la alteración, el uso no autorizado, el robo o el compromiso, cuando exista, de la tarjeta.
- Trasladar a las personas naturales identificadas en el certificado el cumplimiento de las obligaciones específicas de los mismos, y establecer mecanismos para garantizar el efectivo cumplimiento de estas.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de ECLIPSOFT, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación del prestador de servicios de certificación de ECLIPSOFT.

4.5.2.2. RESPONSABILIDAD CIVIL DEL SUSCRIPTOR DE CERTIFICADO

ECLIPSOFT obliga contractualmente al suscriptor a responsabilizarse de:

- Que todas las manifestaciones realizadas en la solicitud son correctas.
- Que todas las informaciones suministradas por el suscriptor que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el suscriptor es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

4.5.3. USO POR EL TERCERO QUE CONFÍA EN CERTIFICADOS

4.5.3.1. OBLIGACIONES DEL TERCERO QUE CONFÍA EN CERTIFICADOS

ECLIPSOFT informa al tercero que confía en certificados de que el mismo debe asumir las siguientes obligaciones:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Verificar la validez, suspensión o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía
- Reconocer que las firmas electrónicas verificadas, son equivalentes a firmas manuscritas.

- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de tercero que confía en el certificado.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de ECLIPSOFT, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación de la ECLIPSOFT.

4.5.3.2. RESPONSABILIDAD CIVIL DEL TERCERO QUE CONFÍA EN CERTIFICADOS

ECLIPSOFT informa al tercero que confía en certificados de que el mismo debe asumir las siguientes responsabilidades:

- Que dispone de suficiente información para tomar una decisión informada con el objeto de confiar en el certificado o no.
- Que es el único responsable de confiar o no en la información contenida en el certificado.
- Que será el único responsable si incumple sus obligaciones como tercero que confía en el certificado.

4.6. RENOVACIÓN DE CERTIFICADOS

4.6.1. VIGENCIA Y NOTIFICACIÓN

Para los certificados emitidos por ECLIPSOFT cuya vigencia sea igual o superior a un (1) año, la Entidad de Certificación enviará una notificación de proximidad de vencimiento al firmante o suscriptor de la firma electrónica asociada al certificado, dicha notificación se cursará con una antelación mínima de treinta (30) días calendario previos a la fecha de caducidad del certificado.

El envío se realizará a través del canal de comunicación previamente acordado con el suscriptor, sin que ello implique responsabilidad para ECLIPSOFT en caso de no recepción por causas imputables al suscriptor o a terceros.

La notificación tiene carácter meramente informativo y no constituye una obligación de renovación automática, siendo responsabilidad exclusiva del suscriptor gestionar la renovación del certificado antes de su vencimiento.

4.6.2. CAMBIO DE CLAVES

ECLIPSOFT no realiza renovaciones de certificados conservando la misma clave privada. Por lo tanto, no se contempla la re-emisión de un certificado vigente o caducado bajo la misma infraestructura de clave.

4.6.3. PROCEDIMIENTO OBLIGATORIO ANTE CADUCIDAD O PRÓXIMA CADUCIDAD

Si el firmante requiere un nuevo certificado de firma electrónica porque el actual ha caducado o se encuentra próximo a caducar, deberá tramitarlo mediante una nueva solicitud, en los mismos términos que una solicitud inicial.

En consecuencia, es obligatorio realizar nuevamente el proceso de identificación y verificación del solicitante, aplicando los mismos criterios y controles exigidos en la solicitud original, sin excepción alguna.

4.7. RENOVACIÓN DE CLAVES Y CERTIFICADOS

4.7.1. CAUSAS DE RENOVACIÓN DE CLAVES Y CERTIFICADOS

Los certificados vigentes se pueden renovar mediante un procedimiento específico y simplificado de solicitud, al efecto de mantener la continuidad del servicio de certificación.

Se consideran al menos dos posibilidades para la renovación de certificados:

- Proceso de renovación, que se efectuará del mismo modo que la emisión de un nuevo certificado.
- Proceso de renovación online (a través de internet), que se detalla a continuación.

4.7.2. PROCEDIMIENTO DE RENOVACIÓN ONLINE DE CERTIFICADOS

a. Notificación: ECLIPSOFT notificará al firmante, vía correo electrónico a la dirección registrada, con al menos 30 días de antelación a la fecha de expiración de su certificado.
b. Solicitud: La renovación debe ser solicitada expresamente por el firmante o el suscriptor a través de la página web de Eclipsoft.
c. Revalidación de Identidad: Se verificará que la identidad del firmante y la vigencia de sus atributos (ej. poderes de representación) se mantienen sin cambios. Si ha habido cambios sustanciales, se requerirá un proceso de registro inicial completo.
d. Generación de Claves: Se generará un nuevo par de claves para el certificado renovado.
e. Emisión del certificado: El titular emitirá el nuevo certificado, con una nueva fecha de expiración y un nuevo número de serie.
f. Estado del Certificado Anterior: El firmante puede obtener su nuevo certificado antes de la caducidad del vigente, en este caso, el certificado anterior se mantiene activo hasta su fecha de vencimiento, salvo que el firmante solicite expresamente su revocación para hacer uso inmediato del nuevo.

La revocación, cuando se solicite, se publicará en la CRL correspondiente, garantizando que no coexistan dos certificados activos para un mismo firmante, de acuerdo con lo establecido por la normativa de ARCOTEL.

4.7.2.1. QUIÉN PUEDE SOLICITAR LA RENOVACIÓN ONLINE DE UN CERTIFICADO

Cualquier firmante podrá pedir la renovación online de su certificado si se cumplen las circunstancias descritas en el punto anterior.

El firmante podrá formalizar su solicitud accediendo al servicio de renovación online de certificados en la página web de ECLIPSOFT.

4.7.2.2. APROBACIÓN O RECHAZO DE LA SOLICITUD

En caso de que los datos se verifiquen correctamente, ECLIPSOFT aprobará la solicitud de renovación del certificado y proceder a su emisión y entrega.

ECLIPSOFT notifica al solicitante la aprobación o denegación de la solicitud.

ECLIPSOFT podrá automatizar los procedimientos de verificación de la corrección de la información que será contenida en los certificados, y de aprobación de las solicitudes.

4.7.2.3. TRAMITACIÓN DE LAS PETICIONES DE RENOVACIÓN ONLINE

La solicitud de una renovación del certificado se realizará de acuerdo con lo siguiente:

- Cuando el certificado electrónico de un usuario esté próximo a caducar, ECLIPSOFT podrá enviar una o más notificaciones distribuidas en el tiempo, invitándole a su renovación.
- El firmante se conectará al servicio de renovación de la página web de ECLIPSOFT y procederá a la solicitud de renovación.
- El firmante firmará la renovación de su certificado válido.
- Se procederá a la generación del nuevo par de claves y generación e importación del certificado, respetando los siguientes condicionantes:
    - Protege la confidencialidad e integridad de los datos de registro de que dispone.
    - Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
    - Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.
    - Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
    - Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
    - Indica la fecha y la hora en que se expidió un certificado.

- Garantiza el control exclusivo del usuario sobre sus propias claves, no pudiendo la propia ECLIPSOFT o sus Entidades de Registro deducirlas o utilizarlas.

4.7.2.4. NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO RENOVADO

ECLIPSOFT notifica la emisión del certificado al suscriptor y a la persona natural identificada en el certificado.

4.7.2.5. CONDUCTA QUE CONSTITUYE ACEPTACIÓN DEL CERTIFICADO RENOVADO

El certificado se considerará aceptado al firmar electrónicamente la renovación.

4.7.2.6. PUBLICACIÓN DEL CERTIFICADO RENOVADO

ECLIPSOFT publica el certificado renovado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes.

4.7.2.7. NOTIFICACIÓN DE LA EMISIÓN A TERCEROS

ECLIPSOFT no realiza notificación alguna de la emisión a terceras entidades.

4.8. MODIFICACIÓN DE CERTIFICADOS

La modificación de certificados, excepto la modificación de la clave pública certificada, que se considera renovación, será tratada como una nueva emisión de certificado, aplicándose lo descrito en las secciones 4.1, 4.2, 4.3 y 4.4.

4.9. REVOCACIÓN, SUSPENSIÓN O REACTIVACIÓN DE CERTIFICADOS

La revocación de un certificado supone la pérdida de validez definitiva del mismo, y es irreversible.

La suspensión (o revocación temporal) de un certificado supone la pérdida de validez temporal del mismo, y es reversible. Sólo los certificados de entidad final podrán ser suspendidos.

La reactivación de un certificado supone su paso de estado suspendido a estado activo.

4.9.1. CAUSAS DE REVOCACIÓN DE CERTIFICADOS

ECLIPSOFT revoca un certificado cuando concurre alguna de las siguientes causas:

1) Circunstancias que afectan a la información contenida en el certificado:
   a) Modificación de alguno de los datos contenidos en el certificado, después de la correspondiente emisión del certificado que incluye las modificaciones.
   b) Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.
   c) Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.
   d) Alteración posterior de las circunstancias verificadas para la expedición del certificado, como por ejemplo las relativas al cargo o facultades.

2) Circunstancias que afectan a la seguridad de la clave o del certificado:
   a) Compromiso de la clave privada, de la infraestructura o de los sistemas del prestador de servicios de certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
   b) Infracción, por ECLIPSOFT, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta Declaración de Prácticas de Certificación.
   c) Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado emitido.
   d) Acceso o utilización no autorizados, por un tercero, de la clave privada correspondiente a la clave pública contenida en el certificado.
   e) El uso irregular del certificado por la persona natural identificada en el certificado, o la falta de diligencia en la custodia de la clave privada.
   f) Utilización de dispositivos cualificados de creación de firma que no cumplen con los estándares de seguridad mínimos y necesarios para garantizar la seguridad del certificado o sus claves privadas.

3) Circunstancias que afectan al suscriptor o a la persona natural identificada en el certificado:
   a) Finalización de la relación jurídica de prestación de servicios entre ECLIPSOFT y el suscriptor.

b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado a la persona natural identificada en el certificado.

c) Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud de este.

d) Infracción por el suscriptor o por la persona identificada en el certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el documento jurídico correspondiente.

e) La incapacidad sobrevenida o el fallecimiento del poseedor de claves.

f) La extinción de la persona jurídica suscriptora del certificado, así como el fin de la autorización del suscriptor al poseedor de claves o la finalización de la relación entre suscriptor y persona identificada en el certificado.

g) Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 3.4.

4) Otras circunstancias:

a) La terminación del servicio de certificación de la Entidad de Certificación de ECLIPSOFT, salvo que de acuerdo con su plan de cese se opte por transferir la gestión de los certificados a otro Prestador de Servicios de Confianza.

b) El incumplimiento de la política de certificación sobre la que ha sido expedido el certificado.

c) Resolución judicial o administrativa que lo ordene.

d) El uso del certificado que sea dañino y continuado para ECLIPSOFT. En este caso, se considera que un uso es dañino en función de los siguientes criterios:

- La naturaleza y el número de quejas recibidas.
- La identidad de las entidades que presentan las quejas.
- La legislación relevante vigente en cada momento.
- La respuesta del suscriptor o de la persona identificada en el certificado a las quejas recibidas.

De acuerdo con lo establecido en el artículo 26 de la Ley de comercio electrónico, firmas electrónicas y mensajes de datos, el certificado de firma electrónica podrá ser revocado por el Consejo Nacional de Telecomunicaciones, de
conformidad con lo previsto en esta Ley, cuando:
a) La Entidad de Certificación de información cese en sus actividades y los certificados vigentes no sean asumidos por otra entidad de certificación; y,
b) Se produzca la quiebra técnica de la entidad de certificación judicialmente declarada. La revocatoria y sus causas deberán ser inmediatamente notificadas al titular del certificado.

4.9.2. CAUSAS DE SUSPENSIÓN DE UN CERTIFICADO

Los certificados de ECLIPSOFT pueden ser suspendidos a partir de las siguientes causas:

- Cuando así sea solicitado por el suscriptor o la persona natural identificada en el certificado.
- Cuando la documentación requerida en la solicitud de revocación sea suficiente pero no se pueda identificar razonablemente al suscriptor o la persona natural identificada en el certificado.
- La falta de uso del certificado durante un periodo prolongado de tiempo, conocido previamente.
- Si se sospecha el compromiso de una clave, hasta que éste sea confirmado. En este caso, ECLIPSOFT tiene que asegurarse de que el certificado no está suspendido durante más tiempo del necesario para confirmar su compromiso.

De acuerdo con lo establecido en el artículo 25 de la Ley de comercio electrónico, firmas electrónicas y mensajes de datos, la Entidad de Certificación de información podrá suspender temporalmente el certificado de firma electrónica cuando:
a) Sea dispuesto por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta Ley;
b) Se compruebe por parte de la entidad de certificación de información, falsedad en los datos consignados por el titular del certificado; y,

c) Se produzca el incumplimiento del contrato celebrado entre la entidad de certificación de información y el titular de la firma electrónica.

La suspensión temporal dispuesta por la entidad de certificación de información deberá ser inmediatamente notificada al titular del certificado y al organismo de control, dicha notificación deberá señalar las causas de la suspensión.

La Entidad de Certificación de información deberá levantar la suspensión temporal una vez desvanecidas las causas que la originaron, o cuando mediare resolución del Consejo Nacional de Telecomunicaciones, en cuyo caso, la entidad de certificación de información está en la obligación de habilitar de inmediato el certificado de firma electrónica.

4.9.3. CAUSAS DE REACTIVACIÓN DE UN CERTIFICADO

Los certificados de ECLIPSOFT pueden ser reactivados a partir de las siguientes causas:

- Cuando el certificado se encuentre en un estado de suspendido.
- Cuando así sea solicitado por el suscriptor o la persona natural identificada en el certificado.

4.9.4. QUIÉN PUEDE SOLICITAR LA REVOCACIÓN, SUSPENSIÓN O REACTIVACIÓN

Pueden solicitar la revocación, suspensión o reactivación de un certificado:

- La persona identificada en el certificado.
- El suscriptor del certificado por medio responsable del servicio de certificación.

4.9.5. PROCEDIMIENTOS DE SOLICITUD DE REVOCACIÓN, SUSPENSIÓN O REACTIVACIÓN

La entidad que precise revocación, suspensión o reactivación de un certificado puede solicitarlo a través de las siguientes vías:

- Directamente contactando con ECLIPSOFT. Los usuarios pueden enviar una petición por correo electrónico o por teléfono, o bien, dirigir un escrito a la dirección social de ECLIPSOFT, según la información proporcionada en el epígrafe 1.5 del presente documento.

- A través de la Entidad de Registro del suscriptor;
- De forma autónoma mediante el servicio en línea disponible en la página web de ECLIPSOFT (https://firmas.eclipsoft.com).

La solicitud de revocación, suspensión o reactivación deberá incorporar la siguiente información:

- Fecha de solicitud de revocación, suspensión o reactivación.
- Identidad del suscriptor.
- Nombre y título de la persona que pide la revocación, suspensión o reactivación.
- Información de contacto de la persona que pide la revocación, suspensión o reactivación.
- Razón detallada para la petición de revocación.

La solicitud debe ser autenticada, por ECLIPSOFT, de acuerdo con los requisitos establecidos en la sección 3.4 de esta política, antes de proceder a la revocación, suspensión o reactivación.
El servicio de revocación, suspensión o reactivación se encuentra en la página web de ECLIPSOFT en la dirección: https://firmas.eclipsoft.com
En caso de que el destinatario de una solicitud de revocación, suspensión o reactivación por parte de una persona natural identificada en el certificado fuera la entidad suscriptora, una vez autenticada la solicitud debe remitir una solicitud en este sentido a ECLIPSOFT.

La solicitud de revocación, suspensión o reactivación será procesada a su recepción, y se informará al suscriptor y, en su caso, a la persona natural identificada en el certificado, acerca del cambio de estado del certificado.
Tanto el servicio de gestión de revocación, suspensión o reactivación como el servicio de consulta son considerados servicios críticos y así constan en el Plan de contingencias y el plan de continuidad de negocio de ECLIPSOFT.
Para garantizar la precisión en los procedimientos de revocación, suspensión o reactivación de certificados, los sistemas involucrados en estos procesos se sincronizan con UTC al menos una vez al día.

4.9.6. PLAZO TEMPORAL DE SOLICITUD DE REVOCACIÓN, SUSPENSIÓN O REACTIVACIÓN

Las solicitudes de revocación, suspensión o reactivación se remitirán de forma inmediata en cuanto se tenga conocimiento.

4.9.7. PLAZO TEMPORAL DE PROCESAMIENTO DE LA SOLICITUD DE REVOCACIÓN, SUSPENSIÓN O REACTIVACIÓN

Las solicitudes de revocación, suspensión o reactivación realizadas a través del servicio online se tramitarán de manera inmediata.

Si la petición se realiza mediante solicitud directa a ECLIPSOFT o a través de un operador de registro, se ejecutará dentro del horario ordinario de operación de ECLIPSOFT o en su caso de la Autoridad de Registro. En cualquier caso, las peticiones se tramitarán en un plazo no superior a 24 horas desde la recepción de la misma.

En el caso de que, debido a una incidencia técnica u operativa, no se pudiere cumplir con el plazo de 24 horas, ECLIPSOFT registrará la solicitud en su sistema de ticketing, asignando un número de caso único, registrando la fecha y hora de recepción de la misma, y designando un responsable para su seguimiento. De igual forma, se indicarán los motivos específicos del retraso, así como las acciones concretas que se llevarán a cabo para asegurar la resolución de la solicitud en el menor tiempo posible.

ECLIPSOFT se pondrá en contacto con el usuario de forma inmediata notificándole:

- Que su solicitud ha sido registrada.
- Información sobre el motivo del retraso.
- Estimación del tiempo para la finalización del proceso

Asimismo, ECLIPSOFT mantendrá al usuario informado del progreso de su solicitud mediante actualizaciones periódicas hasta su resolución. El solicitante podrá ponerse en contacto con ECLIPSOFT a través de los datos de contacto especificados en el epígrafe 1.5.2. del presente documento.

Una vez procesada la solicitud, ECLIPSOFT notificará al usuario, confirmando el resultado de la revocación, suspensión o reactivación.

Finalmente, ECLIPSOFT procederá a cerrar el ticket abierto relacionado con la incidencia.

4.9.8. OBLIGACIÓN DE CONSULTA DE INFORMACIÓN DE REVOCACIÓN O SUSPENSIÓN DE CERTIFICADOS

Los terceros deben comprobar el estado de aquellos certificados en los cuales desean confiar.

Un método por el cual se puede verificar el estado de los certificados es consultando la Lista de Revocación de Certificados más reciente emitida por la Entidad de Certificación de ECLIPSOFT.

Las Listas de Revocación de Certificados se publican en el Depósito de la Entidad de Certificación, así como en las siguientes direcciones web, indicadas dentro de los certificados:

- http://crl1.modernpki.com/tsp/crl/crl_eclipsoft.crl
- http://crl2.modernpki.com/tsp/crl/crl_eclipsoft.crl

El estado de la vigencia de los certificados también se puede comprobar por medio del protocolo OCSP.

- http://ocsp1.modernpki.com/tsp/ocsp/
- https://ocsp2.modernpki.com/tsp/ocsp/

4.9.9. FRECUENCIA DE EMISIÓN DE LISTAS DE REVOCACIÓN DE CERTIFICADOS (LRCS)

ECLIPSOFT emite una LRC al menos cada 24 horas.

La LRC indica el momento programado de emisión de una nueva LRC, si bien se puede emitir una LRC antes del plazo indicado en la LRC anterior, para reflejar revocaciones.

La LRC mantiene obligatoriamente el certificado revocado o suspendido hasta que expira.

Para garantizar la precisión en la gestión de revocación de certificados de la Autoridad de Certificación, los sistemas involucrados en la emisión y publicación de Listas de Revocación de Certificados (LRCs) se sincronizan con UTC al menos una vez al día.

4.9.10. PLAZO MÁXIMO DE PUBLICACIÓN DE LRCS

Las LRCs se publican en el Depósito en un periodo inmediato razonable tras su generación, que en ningún caso no supera unos pocos minutos.

4.9.11. DISPONIBILIDAD DE SERVICIOS DE COMPROBACIÓN EN LÍNEA DE ESTADO DE CERTIFICADOS

De forma alternativa, los terceros que confían en certificados podrán consultar el Depósito de certificados de ECLIPSOFT, que se encuentra disponible las 24 horas de los 7 días.

Para comprobar la última CRL emitida en cada CA se debe descargar:

- *Autoridad de Certificación Raíz (ECLIPSOFT CA ROOT):*
  - http://crl1.modernpki.com/tsp/crl/arl_eclipsoft.crl
  - http://crl2.modernpki.com/tsp/crl/arl_eclipsoft.crl

- *Autoridad de Certificación Intermedia 1 (ECLIPSOFT CA Subordinada 01):*
  - http://crl1.modernpki.com/tsp/crl/crl_eclipsoft.crl
  - http://crl2.modernpki.com/tsp/crl/crl_eclipsoft.crl

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de ECLIPSOFT, ésta deberá realizar sus mejores esfuerzos por asegurar que este servicio se mantenga inactivo el mínimo tiempo posible, que no podrá superar un día.
ECLIPSOFT suministra información a los terceros que confían en certificados acerca del funcionamiento del servicio de información de estado de certificados.

4.9.12. OBLIGACIÓN DE CONSULTA DE SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS

Resulta obligatorio consultar el estado de los certificados antes de confiar en los mismos.

4.9.13. REQUISITOS ESPECIALES EN CASO DE COMPROMISO DE LA CLAVE PRIVADA

El compromiso de la clave privada de ECLIPSOFT es notificado a todos los participantes en los servicios de certificación, en la medida de lo posible, mediante la publicación

de este hecho en la página web de ECLIPSOFT, así como, si se considera necesario, en otros medios de comunicación, incluso en papel.

4.9.14. PERÍODO MÁXIMO DE UN CERTIFICADO ELECTRÓNICO EN ESTADO SUSPENDIDO

El plazo máximo de un certificado electrónico en estado suspendido es indefinido hasta su caducidad.

4.10. FINALIZACIÓN DE LA SUSCRIPCIÓN

Transcurrido el periodo de vigencia del certificado, finalizará la suscripción al servicio. Como excepción, el suscriptor puede mantener el servicio vigente, solicitando la renovación del certificado, con la antelación que determina esta Declaración de Prácticas de Certificación.

ECLIPSOFT puede emitir de oficio un nuevo certificado, mientras los suscriptores mantengan dicho estado.

4.11. DEPÓSITO Y RECUPERACIÓN DE CLAVES

4.11.1. POLÍTICA Y PRÁCTICAS DE DEPÓSITO Y RECUPERACIÓN DE CLAVES

ECLIPSOFT no presta servicios de depósito y recuperación de claves.

4.11.2. POLÍTICA Y PRÁCTICAS DE ENCAPSULADO Y RECUPERACIÓN DE CLAVES DE SESIÓN

Sin estipulación.

5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

5.1. CONTROLES DE SEGURIDAD FÍSICA

Se han establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones para la prestación de los servicios electrónicos de Certificación.

En concreto, la política de seguridad de ECLIPSOFT aplicable a los servicios electrónicos de Certificación establece prescripciones sobre lo siguiente:

- Controles de acceso físico.
- Protección frente a desastres naturales.
- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Protección antirrobo.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

Estas medidas resultan aplicables a las instalaciones desde donde se prestan los servicios electrónicos de Certificación, en sus entornos de producción y contingencia, las cuales son auditadas periódicamente de acuerdo con la normativa aplicable y a las políticas propias de ECLIPSOFT destinadas a este fin.
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.

5.1.1. LOCALIZACIÓN Y CONSTRUCCIÓN DE LAS INSTALACIONES

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta y ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.
La sala donde se realizan las operaciones criptográficas en el Centro de Proceso de Datos cuenta con redundancia en sus infraestructuras, así como varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.
ECLIPSOFT dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados y de gestión de revocación, del

compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de estos.

5.1.2. ACCESO FÍSICO

Se dispone de tres niveles de seguridad física (Entrada del Edificio donde se ubica el CPD, acceso a la sala del CPD y acceso al Rack) para la protección del servicio de generación de certificados, debiendo accederse desde los niveles inferiores a los niveles superiores.

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

- Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro de este, incluyendo filmación por circuito cerrado de televisión y su archivo.
- El acceso a las salas se realiza con lectores de tarjeta de identificación y gestionado por un sistema informático que mantiene un log de entradas y salidas automático.
- Para el acceso al rack donde se ubican los procesos criptográficos es necesario la autorización previa de ECLIPSOFT a los administradores del servicio de hospedaje que disponen de la llave para abrir la jaula.

5.1.3. ELECTRICIDAD Y AIRE ACONDICIONADO

Las instalaciones disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

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

5.1.4. EXPOSICIÓN AL AGUA

Las instalaciones están ubicadas en una zona de bajo riesgo de inundación.

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

5.1.5. PREVENCIÓN Y PROTECCIÓN DE INCENDIOS

Las instalaciones y activos cuentan con sistemas automáticos de detección y extinción de incendios.

5.1.6. ALMACENAMIENTO DE SOPORTES

Únicamente personal autorizado tiene acceso a los medios de almacenamiento.

La información de más alto nivel de clasificación se guarda en una caja de seguridad fuera de las instalaciones del Centro de Proceso de Datos.

5.1.7. TRATAMIENTO DE RESIDUOS

La eliminación de soportes, tanto papel como magnéticos, se realizan mediante mecanismos que garantizan la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se desechan en cuyo caso se destruyen físicamente, o se reutilizan previo proceso de borrado permanente o formateo. En el caso de documentación en papel, mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

5.1.8. COPIA DE RESPALDO FUERA DE LAS INSTALACIONES

Se utiliza un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que son independientes del centro de operaciones.

5.2. CONTROLES DE PROCEDIMIENTOS

Se garantiza que los sistemas se operan de forma segura, para lo cual ha establecido e implantado procedimientos para las funciones que afectan a la provisión de sus servicios.

El personal al servicio de ECLIPSOFT ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

5.2.1.FUNCIONES FIABLES

Se han identificado, de acuerdo con su política de seguridad, las siguientes funciones o roles con la condición de fiables:

- **Auditor Interno:** Responsable del cumplimiento de los procedimientos operativos. Se trata de una persona externa al departamento de Sistemas de Información. Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.
- **Administrador de Sistemas:** Responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación
- **Administrador de CA:** Responsable de las acciones a ejecutar con el material criptográfico, o con la realización de alguna función que implique la activación de las claves privadas de las Entidades de certificación descritas en este documento, o de cualquiera de sus elementos.
- **Operador de CA:** Responsable necesario juntamente con el Administrador de CA de la custodia de material de activación de las claves criptográficas, también responsable de las operaciones de copia de respaldo y mantenimiento de la AC.
- **Operador de Registro:** Persona responsable de aprobar las peticiones de certificación realizadas por el suscriptor y emitir certificados digitales.
- **Oficial de Revocación:** Persona responsable de realizar los cambios en el estado de un certificado, principalmente proceder con la suspensión y revocación de estos.
- **Responsable de Seguridad:** Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de ECLIPSOFT. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos. Adicionalmente, ECLIPSOFT implementa criterios en sus políticas para la segregación de las funciones, como medida de prevención de actividades fraudulentas.

5.2.2. NÚMERO DE PERSONAS POR TAREA

ECLIPSOFT garantiza al menos dos personas para realizar las tareas relativas a la generación, recuperación y back-up de la clave privada de las Autoridades de Certificación. Igual criterio se aplica para la ejecución de tareas de emisión y activación de certificados y claves privadas de las Autoridades de Certificación, y en general cualquier manipulación del dispositivo de custodia de las claves de la Autoridad de Certificación raíz e intermedias.

5.2.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA FUNCIÓN

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurará que cada persona realiza las operaciones para las que está asignado.

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

El acceso a recursos se realiza dependiendo del activo mediante usuario/contraseña, certificado electrónico, tarjeta de acceso físico y/o llaves.

5.2.4. ROLES QUE REQUIEREN SEPARACIÓN DE TAREAS

Las siguientes tareas son realizadas, al menos, por dos personas:

- Las tareas propias del rol de Auditor serán incompatibles con la operación y administración de sistemas, y en general aquellas dedicadas a la prestación directa de los servicios electrónicos de Certificación.
- Emisión y revocación de certificados, serán tareas incompatibles con la Administración y operación de los sistemas.
- La administración y operación de los sistemas y las CAs, serán incompatibles entre sí.

5.2.5. SISTEMA DE GESTIÓN PKI

El sistema de PKI se compone de los siguientes módulos:

- Componente/módulo de gestión de la Autoridad de Certificación Raíz.
- Componente/módulo de gestión de la Autoridad de Certificación Subordinada.
- Componente/módulo de gestión de la Entidad de Registro.

- Componente/módulo de gestión de solicitudes.
- Componente/módulo de gestión de claves (HSM).
- Componente/módulo de bases de datos.
- Componente/módulo de gestión de CRL.
- Componente/módulo de gestión de la Autoridad de Validación (servicios de OCSP).

5.3. CONTROLES DE PERSONAL

5.3.1. REQUISITOS DE HISTORIAL, CALIFICACIONES, EXPERIENCIA Y AUTORIZACIÓN

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

El personal en puestos de Certificación no tiene intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada.

ECLIPSOFT se asegura de que el personal de registro es confiable para realizar las tareas de registro. El Administrador de Registro recibe formación para realizar las tareas de validación de las peticiones.

En general, ECLIPSOFT retirará de sus funciones de Certificación a un empleado cuando se tenga conocimiento de la existencia de conflictos de interés y/o la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.

ECLIPSOFT no asignará a un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por una falta que afecte su idoneidad para el puesto. Por este motivo, previamente se realiza una investigación hasta donde permita la legislación aplicable, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales.
- Referencias profesionales.

En todo caso, las Entidades de Registro podrán establecer procesos de comprobación de antecedentes diferentes, siempre preservando las políticas de ECLIPSOFT, siendo responsables por la actuación de las personas que autoricen en sus operaciones.

5.3.2.PROCEDIMIENTOS DE INVESTIGACIÓN DE HISTORIAL

ECLIPSOFT, antes de contratar a una persona o de que ésta acceda al puesto de trabajo, realiza las siguientes comprobaciones:

- Referencias de los trabajos de los últimos años
- Referencias profesionales
- Estudios, incluyendo titulación alegada.

ECLIPSOFT obtiene el consentimiento inequívoco del afectado para dicha investigación previa, y procesa y protege todos sus datos personales en cumplimiento de la normativa vigente en materia de protección de datos personales.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente aplicable. Los motivos que pueden dar lugar a rechazar al candidato a un puesto fiable son los siguientes:

- Falsedades en la solicitud de trabajo, realizadas por el candidato.
- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato.

5.3.3. REQUISITOS DE FORMACIÓN

ECLIPSOFT forma al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, manteniendo archivo de dicha formación.

Los programas de formación son revisados periódicamente, y son actualizados para su mejor y mejorados de forma periódica.

La formación incluye, al menos, los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.
- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad de ECLIPSOFT. Uso y operación de maquinaria y aplicaciones instaladas.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

5.3.4.REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN FORMATIVA

ECLIPSOFT, actualiza la formación del personal de acuerdo con las necesidades, y con la frecuencia suficiente para cumplir sus funciones de forma competente y satisfactoria, especialmente cuando se realicen modificaciones sustanciales en las tareas de certificación.

5.3.5.SECUENCIA Y FRECUENCIA DE ROTACIÓN LABORAL

No aplicable.

5.3.6.SANCIONES PARA ACCIONES NO AUTORIZADAS

ECLIPSOFT dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, adecuado a la legislación laboral aplicable.
Las acciones disciplinarias incluyen la suspensión, separación de las funciones y hasta el despido de la persona responsable de la acción dañina, de forma proporcionada a la gravedad de la acción no autorizada.

5.3.7.REQUISITOS DE CONTRATACIÓN DE PROFESIONALES

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados por ECLIPSOFT. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían, una vez evaluados, dar lugar al cese del contrato laboral.

En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la Declaración de Prácticas de Certificación, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, no obstante, lo cual, la entidad de certificación será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por tercero distinto a ECLIPSOFT.

5.3.8.SUMINISTRO DE DOCUMENTACIÓN AL PERSONAL

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

5.4. PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

5.4.1.TIPOS DE EVENTOS REGISTRADOS

Se produce y guarda registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- 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 EC a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la EC.
- Encendido y apagado de la aplicación de la EC.
- Cambios en los detalles de la EC y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Creación y revocación de certificados.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de éste.
- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.

- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor, en caso de certificados individuales, o de la persona natural identificada en el certificado, en caso de certificados de organización.
- Posesión de datos de activación, para operaciones con la clave privada de la Entidad de Certificación.
- Eventos relacionados con la sincronización, así como pérdida de esta en lo relativo a las fuentes fiables de tiempo usadas para proporcionar la marca de tiempo en los registros relativos a la Infraestructura de Clave Pública usada por ECLIPSOFT para la prestación de los servicios.
- Eventos relacionados con caídas de los servicios proporcionados mediante la Infraestructura de Clave Pública usada por ECLIPSOFT para la prestación de los servicios.
- Eventos relacionados con la mal función de los equipos usados por ECLIPSOFT en lo relativo a la prestación de servicios de confianza.
- Eventos relacionados con los cortafuegos vinculados a la Infraestructura de Clave Pública usada por ECLIPSOFT para la prestación de los servicios.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.

Las entradas del registro incluyen los siguientes elementos:

- Fecha y hora de la entrada.
- Número de serie o secuencia de la entrada, en los registros automáticos.
- Identidad de la entidad que entra el registro.
- Tipo de entrada.

5.4.2. FRECUENCIA DE TRATAMIENTO DE REGISTROS DE AUDITORÍA

Además de lo anterior, se realiza una revisión de los logs cuando se produce una alerta del sistema motivada por la existencia de algún incidente.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta

o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.

Se mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de logs.
- Que los ficheros de logs no se reescriben.
- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.
- Los ficheros de logs se guardarán en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

5.4.3. PERÍODO DE CONSERVACIÓN DE REGISTROS DE AUDITORÍA

ECLIPSOFT almacena la información de los logs durante un periodo de entre 1 y 15 años, en función del tipo de información registrada.

5.4.4. PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

Los logs de los sistemas:

- Están protegidos de manipulación mediante la firma de los ficheros que los contienen.
- Son almacenados en dispositivos ignífugos.
- Se protege su disponibilidad mediante su almacenamiento en instalaciones externas al centro donde se ubica la EC.

El acceso a los ficheros de logs está reservado solo a las personas autorizadas. Asimismo, los dispositivos son manejados en todo momento por personal autorizado. Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de logs de auditoría.

5.4.5. PROCEDIMIENTOS DE COPIA DE RESPALDO

Se dispone 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.

Sumado a lo anterior, 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. Adicionalmente se mantiene copia en centro de custodia externo.

5.4.6. LOCALIZACIÓN DEL SISTEMA DE ACUMULACIÓN DE REGISTROS DE AUDITORÍA

La información de la auditoria de eventos es recogida internamente y de forma automatizada por el sistema operativo, las comunicaciones de red y por el software de gestión de certificados, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado. Todo ello compone el sistema de acumulación de registros de auditoría.

5.4.7. NOTIFICACIÓN DEL EVENTO DE AUDITORÍA AL CAUSANTE DEL EVENTO

Cuando el sistema de acumulación de registros de auditoría registre un evento, no es preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

5.4.8. ANÁLISIS DE VULNERABILIDADES

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de ECLIPSOFT.

Los análisis de vulnerabilidad deben ser ejecutados, repasadas y revisadas por medio de un examen de estos acontecimientos monitorizados. Estos análisis deben ser ejecutados periódicamente de acuerdo con el procedimiento interno que previsto para este fin.

Los datos de auditoría de los sistemas son almacenados con el fin de ser utilizados en la investigación de cualquier incidencia y localizar vulnerabilidades.

5.5. ARCHIVOS DE INFORMACIONES

ECLIPSOFT, garantiza que toda la información relativa a los certificados se conserva durante un período de tiempo apropiado, según lo establecido en la sección 5.5.2 de esta política.

5.5.1. TIPOS DE REGISTROS ARCHIVADOS

Los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por ECLIPSOFT (o por las entidades de registro):

- Todos los datos de auditoría de sistema.
- Todos los datos relativos a los certificados, incluyendo los contratos con los firmantes y los datos relativos a su identificación y su ubicación
- Solicitudes de emisión y revocación de certificados.
- Tipo de documento presentado en la solicitud del certificado.
- Identidad de la Entidad de Registro que acepta la solicitud de certificado.
- Número de identificación único proporcionado por el documento anterior.
- Todos los certificados emitidos o publicados.
- CRLs emitidas o registros del estado de los certificados generados.
- El historial de claves generadas.
- Las comunicaciones entre los elementos de la PKI.
- Políticas y Prácticas de Certificación
- Todos los datos de auditoría identificados en la sección 5.4
- Información de solicitudes de certificación.
- Documentación aportada para justificar las solicitudes de certificación.
- Información del ciclo de vida del certificado.

ECLIPSOFT y/o las Entidades de Registro según corresponda, serán responsables del correcto archivo de todo este material.

5.5.2. PERÍODO DE CONSERVACIÓN DE REGISTROS

ECLIPSOFT archiva los registros especificados anteriormente durante al menos 15 años, o el período que establezca la legislación vigente.

En particular, los registros de certificados revocados estarán accesibles para su libre consulta durante al menos 15 años o el periodo que establezca la legislación vigente desde su cambio de estado.

5.5.3. PROTECCIÓN DEL ARCHIVO

Se protege el archivo de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo. El archivo es protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable.

Asimismo, se asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en instalaciones seguras externas.

5.5.4. PROCEDIMIENTOS DE COPIA DE RESPALDO

Se dispone 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.

Como mínimo se realizan copias de respaldo incrementales diarias de todos sus documentos electrónicos y realizar copias de respaldo completas semanalmente para casos de recuperación de datos.

Además, ECLIPSOFT (o las organizaciones que realizan la función de registro) guarda copia de los documentos en papel en un lugar seguro diferente de las instalaciones de la propia Entidad de certificación.

5.5.5. REQUISITOS DE SELLADO DE FECHA Y HORA

Los registros están fechados con una fuente fiable vía NTP.

No es necesario que esta información se encuentre firmada digitalmente.

5.5.6. LOCALIZACIÓN DEL SISTEMA DE ARCHIVO

Se dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

5.5.7. PROCEDIMIENTOS DE OBTENCIÓN Y VERIFICACIÓN DE INFORMACIÓN DE ARCHIVO

Se dispone de un procedimiento donde se describe el proceso para verificar que la información archivada es correcta y accesible. ECLIPSOFT proporciona la información y medios de verificación al auditor.

5.6. RENOVACIÓN DE CLAVES

Con anterioridad a que el uso de la clave privada de la EC caduque, será realizado un cambio de claves. La antigua EC y su clave privada solo se usarán para la firma de CRLs mientras existan certificados activos emitidos por dicha EC. Se generará una nueva EC con una clave privada nueva y un nuevo DN. El cambio de claves del suscriptor es realizado mediante la realización de un nuevo proceso de emisión.

Alternativamente, en el caso de Entidades de Certificación subordinadas, se podrá optar por la renovación del certificado con o sin cambio de claves, no resultando aplicable el procedimiento antes descrito.

5.7. COMPROMISO DE CLAVES Y RECUPERACIÓN DE DESASTRE

5.7.1. PROCEDIMIENTOS DE GESTIÓN DE INCIDENCIAS Y COMPROMISOS

ECLIPSOFT ha desarrollado políticas de seguridad y continuidad del negocio que le permiten la gestión y recuperación de los sistemas en caso de incidentes y compromiso de sus operaciones, asegurando los servicios críticos de revocación y publicación del estado de los certificados.

5.7.2. CORRUPCIÓN DE RECURSOS, APLICACIONES O DATOS

Cuando acontezca un evento de corrupción de recursos, aplicaciones o datos, se seguirán los procedimientos de gestión oportunos de acuerdo con las políticas de seguridad y gestión de incidentes de ECLIPSOFT, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los

procedimientos de compromiso de claves o de recuperación de desastres de ECLIPSOFT.

5.7.3. COMPROMISO DE LA CLAVE PRIVADA DE LA ENTIDAD

En caso de sospecha o conocimiento del compromiso de ECLIPSOFT, se activarán los procedimientos de compromiso de claves de acuerdo con las políticas de seguridad, gestión de incidencias y continuidad del negocio, que permita la recuperación de los sistemas críticos, si fuera necesario en un centro de datos alternativo.

5.7.4. CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

ECLIPSOFT restablecerá los servicios críticos (suspensión y revocación, y publicación de información de estado de certificados) de acuerdo con el plan de incidencias y continuidad de negocio existente restaurando la operación normal de los servicios anteriores en las 24 horas siguientes al desastre.

ECLIPSOFT dispone de un centro alternativo en caso de ser necesario para la puesta en funcionamiento de los sistemas de certificación descritos en el plan de continuidad de negocio.

5.8. TERMINACIÓN DEL SERVICIO

ECLIPSOFT asegura que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios del prestador de servicios de certificación. En este sentido, ECLIPSOFT garantiza un mantenimiento continuo de los registros definidos en el apartado 5.5.1, por el tiempo establecido en el apartado 5.5.2 de esta Declaración de Prácticas de Certificación.

No obstante lo anterior, si procede ECLIPSOFT ejecutará todas las acciones que sean necesarias para transferir a un tercero o a un depósito notarial, las obligaciones de mantenimiento de los registros especificados durante el periodo correspondiente según esta Declaración de Prácticas de Certificación o la previsión legal que corresponda.

Antes de terminar sus servicios, ECLIPSOFT desarrolla un plan de terminación, con las siguientes provisiones:

- Proveerá de los fondos necesarios, incluyendo un seguro de responsabilidad civil, para continuar la finalización de las actividades de revocación.
- Informará a todos Firmantes/Suscriptores, Tercero que confían y otras EC con las cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 90 días.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la EC en el procedimiento de emisión de certificados.
- Transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios.
- Dejará en desuso las claves privadas de la EC.
- Mantendrá los certificados activos y el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos.
- Ejecutará las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos durante los períodos de tiempo respectivos indicados al suscriptor y a los terceros que confían en certificados.
- Comunicará al ARCOTEL, con una antelación mínima de 90 días, el cese de su actividad si procede y el destino de los certificados especificando si se transfiere la gestión y a quién o si se extinguirá su vigencia.
- Comunicará, también la apertura de cualquier proceso concursal que se siga contra ECLIPSOFT, así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.

6. CONTROLES DE SEGURIDAD TÉCNICA

ECLIPSOFT emplea sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1.GENERACIÓN DEL PAR DE CLAVES

El par de claves de la entidad de certificación intermedia "ECLIPSOFT CA Subordinada 01" es creada por la entidad de certificación raíz "ECLIPSOFT CA ROOT" de acuerdo con los procedimientos de ceremonia de ECLIPSOFT, dentro del perímetro de alta seguridad destinado a esta tarea.

Las actividades realizadas durante la ceremonia de generación de claves han sido registradas, fechadas y firmadas por todos los individuos participantes en la misma, con la presencia de un Auditor CISA. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado determinado por ECLIPSOFT.

Para la generación de la clave de las entidades de certificación raíz e intermedia se utilizan dispositivos con las certificaciones FIPS 140-2 level 3 y Common Criteria EAL4+.

ECLIPSOFT CA ROOT	4.096 bits	25 años
ECLIPSOFT CA Subordinada 01	4.096 bits	13 años
- Certificados de la Unidad de Sello de tiempo (TSU)	2.048 bits	Hasta 8 años
- Certificados de entidad final	2.048 bits	Hasta 5 años

UANATACA ROOT 2016	4.096 bits	25 años
UANATACA CA1 2016	4.096 bits	13 años
- Certificados de la Unidad de Sello de tiempo (TSU)	2.048 bits	Hasta 8 años
- Certificados de entidad final	2.048 bits	Hasta 5 años

6.1.1.1. GENERACIÓN DEL PAR DE CLAVES DEL FIRMANTE

Las claves del firmante pueden ser generadas por él mismo mediante dispositivos hardware y/o softwares autorizados por ECLIPSOFT. Las claves no generadas en un dispositivo seguro de creación de firma (DSCF), serán generadas por el firmante. ECLIPSOFT nunca genera claves fuera del dispositivo seguro de creación de firma (DSCF) para ser enviadas al firmante.

Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.

6.1.2.ENVÍO DE LA CLAVE PRIVADA AL FIRMANTE

En certificados en dispositivo seguro de creación de firma la clave privada se genera y se almacena debidamente protegida en el interior de dicho dispositivo. En el caso que el dispositivo seguro de creación de firma sea gestionado de manera centralizada, la clave privada del firmante se genera en un área privada del firmante en un HSM remoto. Las credenciales de acceso a la clave privada son introducidas por el propio firmante, no siendo almacenadas ni susceptibles de capacidad de deducción o intercepción por el sistema de generación y custodia remota. La clave privada no se envía al firmante, es decir, nunca abandona el entorno de seguridad que garantiza el control exclusivo de la clave privada por parte del firmante.

En certificados en archivo la clave privada del firmante se genera y se almacena en el sistema informático que utiliza este firmante cuando realiza la solicitud del certificado, por lo que en este caso no existe envío de clave privada, garantizando el control exclusivo de la clave por parte del usuario.

6.1.3.ENVÍO DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

El método de remisión de la clave pública al prestador de servicios electrónicos de Certificación es PKCS#10, otra prueba criptográfica equivalente o cualquier otro método aprobado por ECLIPSOFT.

6.1.4.DISTRIBUCIÓN DE LA CLAVE PÚBLICA DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

Las claves de ECLIPSOFT son comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en el Depósito.

Los usuarios pueden acceder al Depósito para obtener las claves públicas, y adicionalmente, en aplicaciones S/MIME, el mensaje de datos puede contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

El certificado de las Entidades de Certificación Raíz y Subordinada estarán a disposición de los usuarios en la página web de ECLIPSOFT.

6.1.5. TAMAÑOS DE CLAVES

- La longitud de las claves de la Entidad de Certificación raíz es de 4096 bits.
- La longitud de las claves de las Entidad de Certificación subordinada es de 4096 bits.
- La longitud de las claves de los Certificados de Entidad final es de 2048 bits.

6.1.6. GENERACIÓN DE PARÁMETROS DE CLAVE PÚBLICA

La clave pública de la Entidades de Certificación raíz, subordinadas y de los certificados de los suscriptores está codificada de acuerdo con RFC 5280.

Adicionalmente, ECLIPSOFT sigue las directrices de interoperabilidad definidas en el estándar, incluyendo los límites máximos de caracteres en los campos de los certificados. No se han definido restricciones adicionales o más estrictas que las indicadas en RFC 5280.

6.1.7. COMPROBACIÓN DE CALIDAD DE PARÁMETROS DE CLAVE PÚBLICA

- Longitud del Módulo = 4096 bits
- Algoritmo de generación de claves: rsagen1
- Funciones criptográficas de Resumen: SHA256.

6.1.8. GENERACIÓN DE CLAVES EN APLICACIONES INFORMÁTICAS O EN BIENES DE EQUIPO

Todas las claves se generan en bienes de equipo, de acuerdo con lo indicado en la sección 6.1.1.

6.1.9. PROPÓSITOS DE USO DE CLAVES

Los usos de las claves para los certificados de las CA son exclusivamente para la firma de certificados y de CRLs.

Los usos de las claves para los certificados de entidad final son exclusivamente para la firma digital, el no repudio y cifrado de datos.

6.2. PROTECCIÓN DE LA CLAVE PRIVADA

6.2.1. ESTÁNDARES DE MÓDULOS CRIPTOGRÁFICOS

En relación con los módulos que gestionan claves se asegura el nivel exigido por los estándares indicados en las secciones anteriores.

6.2.2. CONTROL POR MÁS DE UNA PERSONA (N DE M) SOBRE LA CLAVE PRIVADA

Se requiere un control multi-persona para la activación de la clave privada de la AC. En el caso de esta Declaración de Prácticas de Certificación, en concreto existe una política de 3 de 6 personas para la activación de las claves.

Los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.

6.2.3. DEPÓSITO DE LA CLAVE PRIVADA

ECLIPSOFT no almacena copias utilizables por medios propios de las claves privadas de los firmantes.

6.2.4. ARCHIVO DE LA CLAVE PRIVADA

Las claves privadas de las AC son archivadas por un periodo de 10 años después de la emisión del último certificado. Se almacenarán en archivos ignífugos seguros y en el centro de custodia externo. Al menos será necesaria la colaboración de dos personas para recuperar la clave privada de las AC en el dispositivo criptográfico inicial.

Solo en caso de certificados de cifrado, el suscriptor podrá almacenar la clave privada el tiempo que crea oportuno. En este caso ECLIPSOFT también guardará copia de la clave privada asociada al certificado de cifrado.

ECLIPSOFT no genera ni archiva claves de certificados, emitidas en archivo.

6.2.5. INTRODUCCIÓN DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

Las claves privadas se generan directamente en los módulos criptográficos de producción de ECLIPSOFT.

6.2.6. MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

Las claves privadas de la Entidad de Certificación se almacenan cifradas en los módulos criptográficos de producción de ECLIPSOFT.

6.2.7. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

La clave privada de ECLIPSOFT se activa mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 6.2.2.

Las claves de la AC se activan por un proceso de m de n (3 de 6).

La activación de las claves privadas de la AC Intermedia es gestionada con el mismo proceso de m de n que las claves de la AC.

6.2.8. MÉTODO DE DESTRUCCIÓN DE LA CLAVE PRIVADA

Para la desactivación de la clave privada de ECLIPSOFT se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.

6.2.9. CLASIFICACIÓN DE MÓDULOS CRIPTOGRÁFICOS

Con anterioridad a la destrucción de las claves, se emitirá una revocación del certificado de las claves públicas asociadas a las mismas.

Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de ECLIPSOFT. Para la eliminación se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.

Finalmente se destruirán de forma segura las copias de seguridad.

Las claves del firmante en archivo se podrán destruir mediante el borrado de las mismas, siguiendo las instrucciones de la aplicación que las alberga.

Las claves del firmante en hardware y podrán ser destruidas mediante una aplicación informática especial en las dependencias de las RA o de ECLIPSOFT.

6.2.10. CLASIFICACIÓN DE MÓDULOS CRIPTOGRÁFICOS

Ver la sección 6.2.1

6.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES

6.3.1. ARCHIVO DE LA CLAVE PÚBLICA

ECLIPSOFT archiva sus claves públicas de forma rutinaria, de acuerdo con lo establecido en la sección 5.5 de este documento.

6.3.2. PERÍODOS DE UTILIZACIÓN DE LAS CLAVES PÚBLICA Y PRIVADA

Los periodos de utilización de las claves son los determinados por la duración del certificado, transcurrido el cual no pueden continuar utilizándose.

Como excepción y en caso de existir, la clave privada de descifrado puede continuar empleándose incluso tras la expiración del certificado.

6.4. DATOS DE ACTIVACIÓN

6.4.1. GENERACIÓN E INSTALACIÓN DE DATOS DE ACTIVACIÓN

Los datos de activación de los dispositivos que protegen las claves privadas de ECLIPSOFT son generados de acuerdo con lo establecido en la sección 6.2.2 y los procedimientos de ceremonia de claves.

La creación y distribución de dichos dispositivos es registrada.

Asimismo, ECLIPSOFT genera de forma segura los datos de activación.

6.4.2. PROTECCIÓN DE DATOS DE ACTIVACIÓN

Los datos de activación de los dispositivos que protegen las claves privadas de las Entidades de certificación raíz y subordinadas, están protegidos por los poseedores de las tarjetas de administradores de los módulos criptográficos, según consta en el documento de ceremonia de claves.

El firmante del certificado es el responsable de la protección de su clave privada, con una o varias contraseñas lo más completas y complejas posible. El firmante debe recordar dicha(s) contraseña(s).

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

Se emplean sistemas fiables para ofrecer sus servicios de certificación. Para atender a este fin, se han implementado controles y auditorias informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información, la Infraestructura de Clave Pública aplica los controles del esquema de certificación sobre sistemas de gestión de la información ISO 27001.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de ECLIPSOFT, 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.
- Configuración antivirus.
- Requerimientos de tráfico de red.

6.5.1. REQUISITOS TÉCNICOS ESPECÍFICOS DE SEGURIDAD INFORMÁTICA

Cada servidor de incluye las siguientes funcionalidades:

- Control de acceso a los servicios de las Entidades de Certificación subordinadas 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, de las Entidades de Certificación subordinadas y datos de auditoría.
- Auditoria de eventos relativos a la seguridad.
- Auto-diagnóstico de seguridad relacionado con los servicios de las Entidades de Certificación subordinadas.
- Mecanismos de recuperación de claves y del sistema de las Entidades de Certificación subordinadas.

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

6.5.2. EVALUACIÓN DEL NIVEL DE SEGURIDAD INFORMÁTICA

Las aplicaciones de Entidad de certificación y de registro empleadas por ECLIPSOFT son fiables.

6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA

6.6.1. CONTROLES DE DESARROLLO DE SISTEMAS

Las aplicaciones son desarrolladas e implementadas por ECLIPSOFT de acuerdo con estándares de desarrollo y control de cambios.

Las aplicaciones disponen de métodos para la verificación de la integridad y autenticidad, así como de la corrección de la versión a emplear.

6.6.2. CONTROLES DE GESTIÓN DE SEGURIDAD

ECLIPSOFT desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un grupo para la gestión de la seguridad. En la realización de esta función dispone de un plan de formación anual.

ECLIPSOFT exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de servicios electrónicos de Certificación.

6.6.2.1. CLASIFICACIÓN Y GESTIÓN DE INFORMACIÓN Y BIENES

ECLIPSOFT mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad de ECLIPSOFT detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en cuatro niveles: SIN CLASIFICAR, PÚBLICO, USO INTERNO y CONFIDENCIAL.

6.6.2.2. OPERACIONES DE GESTIÓN

ECLIPSOFT dispone 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 el documento de seguridad de ECLIPSOFT se desarrolla en detalle el proceso de gestión de incidencias.

ECLIPSOFT tiene 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.

6.6.2.3. TRATAMIENTO DE LOS SOPORTES Y SEGURIDAD

Todos los soportes son 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.

Planificación del sistema

El departamento de Sistemas de ECLIPSOFT mantiene un registro de las capacidades de los equipos. Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

Reportes de incidencias y respuesta

ECLIPSOFT dispone 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.

Procedimientos operacionales y responsabilidades

ECLIPSOFT define actividades, asignadas a personas con un rol de Certificación, distintas de las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

6.6.2.4. GESTIÓN DEL SISTEMA DE ACCESO

ECLIPSOFT realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.
En particular:

AC General

- Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.
- ECLIPSOFT dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- ECLIPSOFT dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.
- Cada persona tiene asociado un rol para realizar las operaciones de certificación.
- El personal de ECLIPSOFT es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

Generación del certificado

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

Gestión de la revocación

La revocación se realizará mediante autenticación fuerte a las aplicaciones de un administrador autorizado. Los sistemas de logs generarán las pruebas que garantizan el no repudio de la acción realizada por el administrador de ECLIPSOFT.

Estado de la revocación

La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación con certificados o con doble factor de identificación para evitar el intento de modificación de la información del estado de la revocación.

6.6.2.5. GESTIÓN DEL CICLO DE VIDA DEL HARDWARE CRIPTOGRÁFICO

ECLIPSOFT se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte mediante la inspección del material entregado.

El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación.

ECLIPSOFT registra toda la información pertinente del dispositivo para añadir al catálogo de activos.

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

ECLIPSOFT realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo hardware criptográfico solo es manipulado por personal confiable.

La clave privada de firma de ECLIPSOFT almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

La configuración del sistema de ECLIPSOFT, así como sus modificaciones y actualizaciones son documentadas y controladas.

Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

6.7. CONTROLES DE SEGURIDAD DE RED

ECLIPSOFT protege el acceso físico a los dispositivos de gestión de red, y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad, creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se trasfiere por redes no seguras, se realiza de forma cifrada mediante uso de protocolos SSL o del sistema VPN con autenticación por doble factor.

6.8. CONTROLES DE INGENIERÍA DE MÓDULOS CRIPTOGRÁFICOS

Los módulos criptográficos se someten a los controles de ingeniería previstos en las normas indicadas a lo largo de esta sección.

Los algoritmos de generación de claves empleados se aceptan comúnmente para el uso de la clave a que están destinados.

Todas las operaciones criptográficas de ECLIPSOFT son realizadas en módulos con las certificaciones FIPS 140-2 nivel 3.

6.9. FUENTES DE TIEMPO

ECLIPSOFT tiene un procedimiento de sincronización de tiempo coordinado vía NTP, que accede a dos servicios independientes:

La primera sincronización es con un servicio basado en antenas y receptores GPS que permite un nivel de Certificación de STRATUM 1 (con dos sistemas en alta disponibilidad).

La segunda dispone de una sincronización complementaria, vía NTP, con el Real Instituto y Observatorio de la Armada (ROA)

6.10. CAMBIO DE ESTADO DE UN DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA (DSCF)

ECLIPSOFT en el caso de modificación del estado de la certificación de los dispositivos seguros de creación de firma (DSCF), procederá de la siguiente manera:

1. ECLIPSOFT dispone de una lista de varios DSCF certificados, así como una estrecha relación con proveedores de dichos dispositivos, con el fin de garantizar alternativas a posibles pérdidas de estado de certificación de dispositivos DSCF.
2. En el supuesto de finalización del periodo de validez o pérdida de la certificación, ECLIPSOFT no utilizará dichos DSCF para la emisión de nuevos certificados

digitales, bien sea en nuevas emisiones como eventualmente en posibles renovaciones.

3. Procederá de inmediato a cambiar a de dispositivos DSCF con certificación válida.
4. En el supuesto caso que un dispositivo DSCF haya demostrado no haberlo sido nunca, por falsificación o cualquier otro tipo de fraude, ECLIPSOFT procederá de inmediato a comunicárselo a sus clientes y al ente regulador, revocar los certificados digitales emitidos en estos dispositivos y reemplazarlos emitiéndolos en DSCF válidos

7. PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS

7.1. PERFIL DE CERTIFICADO

Todos los certificados emitidos bajo esta política cumplen con el estándar X.509 versión 3, el RFC 3739 y los diferentes perfiles descritos en la norma EN 319 412.

7.1.1.NÚMERO DE VERSIÓN

ECLIPSOFT emite certificados X.509 Versión 3

7.1.2.EXTENSIONES DEL CERTIFICADO

Las extensiones de los certificados se encuentran desarrolladas en los propios certificados.

7.1.3.IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS

El identificador de objeto del algoritmo de firma es:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

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

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4. FORMATO DE NOMBRES

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política.

7.1.5. RESTRICCIÓN DE LOS NOMBRES

Los nombres contenidos en los certificados están restringidos a "Distinguished Names" X.500, que son únicos y no ambiguos.

7.1.6. IDENTIFICADOR DE OBJETO (OID) DE LOS TIPOS DE CERTIFICADOS

Todos los certificados incluyen un identificador de política de certificados bajo la que han sido emitidos, de acuerdo con la estructura indicada en el punto 1.3.1

7.2. PERFIL DE LA LISTA DE REVOCACIÓN DE CERTIFICADOS

7.2.1. NÚMERO DE VERSIÓN

Las CRL emitidas por ECLIPSOFT son de la versión 2.

7.2.2. PERFIL DE OCSP

Según el estándar IETF RFC 6960.

8. AUDITORÍA DE CONFORMIDAD

ECLIPSOFT ha comunicado el inicio de su actividad como prestador de servicios de certificación a ARCOTEL se encuentra sometida a las revisiones de control que este organismo considere necesarias.

8.1. FRECUENCIA DE LA AUDITORÍA DE CONFORMIDAD

ECLIPSOFT lleva a cabo una auditoría de conformidad anualmente, además de las auditorías internas que realiza bajo su propio criterio o en cualquier momento, debido a una sospecha de incumplimiento de alguna medida de seguridad.

8.2. IDENTIFICACIÓN Y CALIFICACIÓN DEL AUDITOR

Las auditorías de conformidad, necesarias para verificar el cumplimiento de lo establecido en esta DPC y la normativa legal aplicable, serán realizadas por una entidad auditora externa independiente. Dicha entidad deberá cumplir con los siguientes requisitos, en línea con lo exigido por ARCOTEL:

- Estar debidamente acreditada por el organismo nacional de acreditación para la realización de auditorías.
- Ser reconocida y aceptada por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) como entidad apta para auditar Prestadores de Servicios de Certificación.
- El equipo auditor deberá demostrar competencia técnica y experiencia demostrable en seguridad de infraestructuras de clave pública (PKI), criptografía y auditoría de servicios de confianza.

8.3. RELACIÓN DEL AUDITOR CON LA ENTIDAD AUDITADA

Las empresas de auditoría son de reconocido prestigio con departamentos especializados en la realización de auditorías informáticas, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación en relación con ECLIPSOFT.

8.4. LISTADO DE ELEMENTOS OBJETO DE AUDITORÍA

La auditoría verifica respecto a ECLIPSOFT:

a) Que la entidad tiene un sistema de gestión que garantiza la calidad del servicio prestado.
b) Que la entidad cumple con los requerimientos de la Declaración de Prácticas de Certificación y otra documentación vinculada con la emisión de los distintos certificados digitales.
c) Que la Declaración de Prácticas de Certificación y demás documentación jurídica vinculada, se ajusta a lo acordado por ECLIPSOFT y con lo establecido en la normativa vigente.
d) Que la entidad gestiona de forma adecuada sus sistemas de información.

En particular, los elementos objeto de auditoría serán los siguientes:

a) Procesos de las Entidades de Certificación, Entidades de Registro y elementos relacionados.
b) Sistemas de información.
c) Protección del centro de proceso de datos.
d) Documentos.

8.5. ACCIONES A EMPRENDER COMO RESULTADO DE UNA FALTA DE CONFORMIDAD

Una vez recibido por la dirección el informe de la auditoría de cumplimiento realizada, se analizan, con la firma que ha ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta las medidas correctivas que solventen dichas deficiencias.

Si ECLIPSOFT es incapaz de desarrollar y/o ejecutar las medidas correctivas o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, deberá comunicarlo inmediatamente al Comité de Seguridad de ECLIPSOFT que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Revocar la clave de la Entidad de Certificación y regenerar la infraestructura.
- Terminar el servicio de la Entidad de Certificación.
- Otras acciones complementarias que resulten necesarias.

8.6. TRATAMIENTO DE LOS INFORMES DE AUDITORÍA

En cumplimiento de la normativa aplicable, ECLIPSOFT se somete anualmente a una auditoría externa de Seguridad Informática, una vez finalizado y recibido el informe final, se procederá de la siguiente manera:

1. Análisis Interno: La dirección de ECLIPSOFT y el Comité de Seguridad analizarán el informe y las no conformidades u observaciones planteadas, desarrollando un plan de acciones correctivas si fuera necesario.

2. Comunicación a ARCOTEL: En cumplimiento del plazo establecido en la normativa técnica vigente, ECLIPSOFT remitirá el informe de auditoría a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) en un plazo no mayor a 15 días hábiles, contados a partir de la fecha de emisión del informe por parte de la entidad auditora.

9. REQUISITOS COMERCIALES Y LEGALES

9.1. TARIFAS

9.1.1. TARIFA DE EMISIÓN O RENOVACIÓN DE CERTIFICADOS

ECLIPSOFT pone a disposición de sus clientes las siguientes tarifas aplicables a los servicios de certificación expresadas en dólares de los Estados Unidos de América. Los valores se presentan sin incluir el Impuesto al Valor Agregado (IVA) del 15%, de conformidad con la normativa tributaria vigente y publicado en la página https://firmas.eclipsoft.com/

Servicios por tipo de certificado y vigencia	Vigencia	Subtotal (No incluye IVA)
Emisión o renovación de certificado de firma electrónica en archivo o nube ▪ Persona natural ▪ Miembro de empresa ▪ Representante Legal ▪ Sello Electrónico	7 días	$4,35
Emisión o renovación de certificado de firma electrónica en archivo o nube ▪ Persona natural ▪ Miembro de empresa ▪ Representante Legal ▪ Sello Electrónico	90 días	$8,70
Emisión o renovación de certificado de firma electrónica en archivo o nube ▪ Persona natural ▪ Miembro de empresa ▪ Representante Legal ▪ Sello Electrónico	1 año	$17,39
Emisión o renovación de certificado de firma electrónica en archivo o nube ▪ Persona natural ▪ Miembro de empresa	2 años	$23,48

▪ Representante Legal ▪ Sello Electrónico		
Emisión o renovación de certificado de firma electrónica en archivo o nube ▪ Persona natural ▪ Miembro de empresa ▪ Representante Legal ▪ Sello Electrónico	3 años	$37,39
Sellado de tiempo electrónico		$0.02

Forma de pago: Transferencias, depósito y pagos con tarjeta de crédito y débito

ECLIPSOFT, en el marco de su autonomía comercial, podrá implementar campañas promocionales o programas de fidelización que contemplen descuentos sobre las tarifas establecidas. Dichas iniciativas serán aplicadas a criterio exclusivo de la entidad, y el precio resultante corresponderá al valor tarifario vigente menos el descuento ofertado. Las condiciones particulares de cada promoción serán oportunamente divulgadas a través de la página web institucional y de los canales de atención al firmante.

9.1.2. TARIFA DE ACCESO A CERTIFICADOS

ECLIPSOFT no ha establecido ninguna tarifa por el acceso a los certificados.

Servicio	Tipo de certificado / servicio	Subtotal (No incluye IVA)
Consulta de estado (OCSP / CRL)	Todos los certificados Todos los servicios	$0.00

9.1.3. TARIFA DE ACCESO A INFORMACIÓN DE ESTADO DE CERTIFICADO

ECLIPSOFT no ha establecido ninguna tarifa por el acceso a la información de estado de certificados.

Servicio	Tipo de certificado / servicio	Subtotal (No incluye IVA)
Consulta de estado (OCSP / CRL)	Todos los certificados Todos los servicios	$0.00

9.1.4. TARIFAS DE OTROS SERVICIOS

No aplica / conforme condiciones contractuales.

9.1.5. POLÍTICA DE REINTEGRO

No aplica / conforme condiciones contractuales.

9.2. CAPACIDAD FINANCIERA

ECLIPSOFT dispone de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios

9.2.1. COBERTURA DE SEGURO

ECLIPSOFT dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional, que mantiene de acuerdo con la normativa vigente aplicable.

9.2.2. OTROS ACTIVOS

Sin estipulación.

9.2.3. COBERTURA DE SEGURO PARA SUSCRIPTORES Y TERCEROS QUE CONFÍAN EN CERTIFICADOS

ECLIPSOFT dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional, para los servicios electrónicos de Certificación atendiendo al mínimo establecido por la legislación del Ecuador.

9.3. CONFIDENCIALIDAD

9.3.1.INFORMACIONES CONFIDENCIALES

Las siguientes informaciones son mantenidas confidenciales por ECLIPSOFT:

- 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 la sección siguiente.
- Claves privadas generadas y/o almacenadas por el prestador de servicios de certificación.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por la Entidad de Certificación y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Planes de seguridad.
- Documentación de operaciones, archivo, monitorización y otros análogos.
- Toda otra información identificada como "Confidencial".

9.3.2. INFORMACIONES NO CONFIDENCIALES

La siguiente información se considera no confidencial:

- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por la Entidad de Certificación.
- El nombre y los apellidos de la persona natural identificada en el certificado, así como cualquiera otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
- La dirección de correo electrónico de la persona natural identificada en el certificado, o la dirección de correo electrónico asignada por el suscriptor, en el supuesto de que sea significativa en función de la finalidad del certificado.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.

- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (LRCs), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- Cualquier otra información que no esté indicada en la sección anterior.

9.3.3. DIVULGACIÓN DE INFORMACIÓN DE SUSPENSIÓN Y REVOCACIÓN

Véase la sección anterior.

9.3.4. DIVULGACIÓN LEGAL DE INFORMACIÓN

ECLIPSOFT divulga la información confidencial únicamente en los casos legalmente previstos.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado serán divulgados en caso de ser requerido para ofrecer evidencia de la certificación en un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

ECLIPSOFT indicará estas circunstancias en la política de privacidad prevista en la sección 9.4.

9.3.5. DIVULGACIÓN DE INFORMACIÓN POR PETICIÓN DE SU TITULAR

ECLIPSOFT incluye, en la política de privacidad prevista en la sección 9.4, prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, de la persona natural identificada en el certificado, directamente a los mismos o a terceros.

9.3.6. OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

Sin estipulación.

9.4. PROTECCIÓN DE DATOS PERSONALES

ECLIPSOFT garantiza el cumplimiento de la normativa vigente en cada momento en materia de protección de datos personales, documentando en la presente Declaración de Prácticas de Certificación, todos los aspectos, procesos y procedimientos de seguridad correspondientes respecto de los datos de los usuarios.

Los datos de los usuarios serán usados única y exclusivamente para los fines indicados en el presente documento. No se procederá a la divulgación o cesión de los datos personales salvo en los casos previstos en esta DPC.

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

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

9.5.1. PROPIEDAD DE LOS CERTIFICADOS E INFORMACIÓN DE REVOCACIÓN

Únicamente ECLIPSOFT goza de derechos de propiedad intelectual sobre los certificados que emita, sin perjuicio de los derechos de los suscriptores, poseedores de claves y terceros, a los que conceda licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de uso del certificado, y de acuerdo con la documentación que los vincula.

Adicionalmente, los certificados emitidos por ECLIPSOFT contienen un aviso legal relativo a la propiedad de estos.

Las mismas reglas resultan de aplicación al uso de la información de revocación de los certificados.

9.5.2. PROPIEDAD DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Únicamente ECLIPSOFT goza de derechos de propiedad intelectual sobre esta Declaración de Prácticas de Certificación.

9.5.3. PROPIEDAD DE LA INFORMACIÓN RELATIVA A NOMBRES

El suscriptor y, en su caso, la persona natural identificada en el certificado conserva la totalidad de derechos, de existir los mismos, sobre la marca, producto o nombre comercial contenido en el certificado.

El suscriptor es el propietario del nombre distinguido (DN) del certificado, formado por las informaciones especificadas en la sección 3.1.1.

9.5.4. PROPIEDAD DE CLAVES

Los pares de claves son propiedad de los de los certificados.

Cuando una clave se encuentra fraccionada en partes, todas las partes de la clave son propiedad del propietario de la clave.

9.6. OBLIGACIONES Y RESPONSABILIDAD CIVIL

9.6.1. OBLIGACIONES DE ECLIPSOFT

ECLIPSOFT garantiza, bajo su plena responsabilidad, que cumple con la totalidad de los requisitos establecidos en la Declaración de Prácticas de Certificación, siendo el responsable del cumplimiento de los procedimientos descritos, de acuerdo con las indicaciones contenidas en este documento.

ECLIPSOFT presta los servicios electrónicos de Certificación conforme con esta Declaración de Prácticas de Certificación.

ECLIPSOFT informa al suscriptor de los términos y condiciones relativos al uso del certificado, de su precio y de sus limitaciones de uso, mediante un contrato de suscriptor.

- Prescripciones para dar cumplimiento a lo establecido en las secciones 4.5.3, 9.2, 9.6.7, 9.6.8, 9.6.9 y 9.6.10.
- Indicación de la política aplicable, con indicación de que los certificados no se expiden al público.
- Manifestación de que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
- Consentimiento para la publicación del certificado en el depósito y acceso por terceros al mismo.

- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor y para la cesión de dicha información a terceros, en caso de terminación de operaciones de la Entidad de Certificación sin revocación de certificados válidos.
- Límites de uso del certificado, incluyendo las establecidas en la sección 1.5.2
- Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado, que resulta aplicable cuando el suscriptor actúa como tercero que confía en el certificado.
- Forma en que se garantiza la responsabilidad patrimonial de la Entidad de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Entidad de Certificación acepta o excluye su responsabilidad.
- Periodo de archivo de información de solicitud de certificados.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas, disponible en: https://firmas.eclipsoft.com.
- Ley aplicable y jurisdicción competente.
- Si la Entidad de Certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

9.6.2. GARANTÍAS OFRECIDAS A SUSCRIPTORES Y TERCEROS QUE CONFÍAN EN CERTIFICADOS

ECLIPSOFT, en la documentación que la vincula con suscriptores y terceros que confían en certificados, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

ECLIPSOFT, como mínimo, garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Entidad de Certificación.
- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de la diligencia debida en la gestión de la solicitud de certificado o en la creación de este.

- Que los certificados cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.
- Que los servicios de revocación y el empleo del Depósito cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.

ECLIPSOFT, como mínimo, garantizará al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- En caso de certificados publicados en el Depósito, que el certificado ha sido emitido al suscriptor identificado en el mismo y que el certificado ha sido aceptado, de acuerdo con la sección 4.4.
- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y Depósito.

Adicionalmente, ECLIPSOFT garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado según lo dispuesto en la legislación ecuatoriana a tal efecto así como respecto de lo indicado en la presente Declaración de Practicas de Certificación.
- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, persona natural identificada en el certificado, se mantiene su confidencialidad durante el proceso.
- La responsabilidad de la Entidad de Certificación, con los límites que se establezcan.

9.6.3.RECHAZO DE OTRAS GARANTÍAS

ECLIPSOFT rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección 9.6.2.

9.6.4.LIMITACIÓN DE RESPONSABILIDADES

ECLIPSOFT, en su calidad de Entidad de Certificación Acreditada, asume responsabilidad únicamente por los actos y omisiones que le sean directamente imputables en la emisión, gestión y revocación de los certificados electrónicos y de los pares de claves que genera. La responsabilidad económica por concepto de indemnización se limita a los montos máximos establecidos para cada tipo de certificado, según se detalla a continuación, en estricta correspondencia con lo estipulado en el Acuerdo de Suscriptor (RSA) suscrito entre las partes:

Límites máximos de responsabilidad económica ECLIPSOFT indemnizará hasta el 100% de la tarifa del Certificado de Firma Electrónica emitido al firmante/Suscriptor.		
Tipo de certificado	**Límite máx. de indemnización (USD)**	**Referencia**
Certificado de firma electrónica en archivo o nube de 7 días ▪ Persona natural ▪ Miembro de empresa ▪ Representante Legal ▪ Sello Electrónico	$5.00	Contrato de prestación de servicios de certificación – Cláusula 5. Régimen de Responsabilidad y Ejecución de Garantía
Certificado de firma electrónica en archivo o nube de 90 días ▪ Persona natural ▪ Miembro de empresa ▪ Representante Legal ▪ Sello Electrónico	$10.00	Contrato de prestación de servicios de certificación – Cláusula 5. Régimen de Responsabilidad y Ejecución de Garantía
Certificado de firma electrónica en archivo o nube de 1 año ▪ Persona natural ▪ Miembro de empresa ▪ Representante Legal ▪ Sello Electrónico	$20.00	Contrato de prestación de servicios de certificación – Cláusula 5. Régimen de Responsabilidad y Ejecución de Garantía

Certificado de firma electrónica en archivo o nube de 2 años ▪ Persona natural ▪ Miembro de empresa ▪ Representante Legal ▪ Sello Electrónico	$27.00	Contrato de prestación de servicios de certificación – Cláusula 5. Régimen de Responsabilidad y Ejecución de Garantía
Certificado de firma electrónica en archivo o nube de 3 años ▪ Persona natural ▪ Miembro de empresa ▪ Representante Legal ▪ Sello Electrónico	$43.00	Contrato de prestación de servicios de certificación – Cláusula 5. Régimen de Responsabilidad y Ejecución de Garantía
Selllado de tiempo	$0.02	Contrato de prestación de servicios de certificación – Cláusula 5. Régimen de Responsabilidad y Ejecución de Garantía

*Valores no incluyen IVA

Estos límites constituyen el máximo resarcimiento que ECLIPSOFT podrá ser obligada a pagar en favor del firmante o de terceros afectados, derivado de cualquier reclamación judicial o extrajudicial relacionada con el uso, emisión, suspensión o revocación del certificado, siempre que se acredite fehacientemente un daño directo causado por incumplimiento de las obligaciones legales o contractuales imputables a ECLIPSOFT.

Los referidos montos se aplican por cada certificado individualmente considerado y por cada evento de incumplimiento. En ningún caso la responsabilidad total acumulada excederá el límite correspondiente al tipo de certificado reclamado, independientemente del número de perjuicios alegados o de la pluralidad de reclamantes.

No se asume responsabilidad por usos indebidos, decisiones de confianza sin verificación de estado (OCSP/CRL) o incumplimientos del suscriptor/tercero.

Las condiciones aquí previstas se encuentran debidamente reflejadas en el Acuerdo de Suscriptor (RSA) que rige la relación entre ECLIPSOFT y el firmante, garantizando la coherencia jurídica y la transparencia en los términos de responsabilidad asumidos.

En la máxima extensión permitida por la normativa aplicable, en particular por el ordenamiento jurídico ecuatoriano y las disposiciones emitidas por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), no serán aplicables –por no estar previstos o por resultar contrarios a las condiciones contractuales establecidas en la presente DPC– los siguientes conceptos ni aquellos que deriven de ellos:

- Daños indirectos o consecuenciales
- Lucro cesante o pérdida de ganancias
- Pérdida de oportunidad de negocio
- Pérdida, corrupción o inaccesibilidad de datos

- Interrupción de la actividad comercial o del servicio
- Reclamaciones de terceros

Lo anterior se aplica únicamente cuando dichos daños o reclamaciones se deriven del uso del certificado digital fuera de los términos y condiciones expresamente contemplados en esta DPC, incluyendo, entre otros, los supuestos de uso no autorizado, incumplimiento de los deberes del suscriptor o aplicación del certificado en contextos no permitidos por la acreditación otorgada por ARCOTEL.

9.6.5.CLÁUSULAS DE INDEMNIDAD

9.6.5.1. CLÁUSULA DE INDEMNIDAD DE SUSCRIPTOR

ECLIPSOFT incluye en el contrato con el suscriptor, una cláusula por la cual el suscriptor se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Falsedad o manifestación errónea realizada por el usuario del certificado.
- Error del usuario del certificado al facilitar los datos de la solicitud, si en la acción u omisión medió dolo o negligencia con respecto a la Entidad de Certificación o a cualquier persona que confía en el certificado.
- Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.
- Empleo por el suscriptor de un nombre (incluyendo nombres comunes, dirección de correo electrónico y nombres de domino), u otras informaciones en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.

9.6.5.2. CLÁUSULA DE INDEMNIDAD DE TERCERO QUE CONFÍA EN EL CERTIFICADO

ECLIPSOFT incluye una cláusula por la cual el tercero que confía en el certificado se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Certificación temeraria en un certificado, a tenor de las circunstancias.
- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.

9.6.6.CASO FORTUITO Y FUERZA MAYOR

ECLIPSOFT incluye cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

9.6.7.LEY APLICABLE

ECLIPSOFT establece, en el contrato de suscriptor, que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la ley de la República del Ecuador.

9.6.8.CLÁUSULAS DE DIVISIBILIDAD, SUPERVIVENCIA, ACUERDO ÍNTEGRO Y NOTIFICACIÓN

ECLIPSOFT establece, en el contrato de suscriptor, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, la Entidad de Certificación vela porque, al menos los requisitos contenidos en las secciones 9.6.1 (Obligaciones y responsabilidad), 8 (Auditoría de conformidad) y 9.3 (Confidencialidad), continúen vigentes tras la terminación del servicio y de las condiciones generales de emisión/uso.
- En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

9.6.9.CLÁUSULA DE JURISDICCIÓN COMPETENTE

ECLIPSOFT establece, en el contrato de suscriptor una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces del Ecuador.

La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

9.6.10. RESOLUCIÓN DE CONFLICTOS

ECLIPSOFT establece, en el contrato de suscriptor, los procedimientos de mediación y resolución de conflictos aplicables.

10. REVISIÓN Y APROBACIÓN

Documento revisado por:

VERSIÓN:	FECHA:	NOMBRE	CARGO
1	24/03/2023	Ma. Belén Macías	Jefe PPC
2	10/12/2025	Maria Belen Macias	Jefe de Calidad y Cumplimiento Normativo (CCN)
3	16/04/2026	Maria Belen Macias	Jefe de Calidad y Cumplimiento Normativo (CCN)

Documento aprobado por:

VERSIÓN:	FECHA:	NOMBRE	CARGO
1	24/03/2023	Ma. Belén Macías	Jefe PPC
2	10/12/2025	José Caballero	Gerente General
3	16/04/2026	José Caballero	Gerente General

11. ANEXO I – ACRÓNIMOS

EBA	Autoridad Bancaria Europea
AC	Autoridad de Certificación
CA	Certification Authority. Autoridad de Certificación
RA	Autoridad de Registro
NCA	Autoridad Nacional Competente (PSD2)
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List Lista de certificados revocados
CSR	Certificate Signing Request Petición de firma de certificado
DES	Data Encryption Standard Estándar de cifrado de datos
DN	Distinguished Name Nombre distintivo dentro del certificado digital
DPC	Declaración de Prácticas de Certificación
DSA	Digital Signature Algorithm Estándar de algoritmo de firma
DSCF	Dispositivo Seguro de Creación de Firma
FIPS	Federal Information Processing Standard Publication
ISO	International Organization for Standardization Organismo Internacional de Estandarización
LDAP	Lightweight Directory Access Protocol Protocolo de acceso a directorios

OCSP	On-line Certificate Status Protocol Protocolo de acceso al estado de los certificados
OID	Object Identifier Identificador de objeto
PA	Policy Authority Autoridad de Políticas
PC	Política de Certificación
PIN	Personal Identification Number Número de identificación personal
PKI	Public Key Infrastructure Infraestructura de clave pública
RSA	Rivest-Shimar-Adleman Tipo de algoritmo de cifrado
SHA	Secure Hash Algorithm Algoritmo seguro de Hash
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol