Certificamos Información Digital

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)	
SGSI - GG	Código: **DPC-DES-DC-00013**
	Versión: 2.0
	Clasificación de Información: Documento de Acceso Público

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DICERT (DPC)

Aprobado por:	**Firma de Aprobación:**
Galo Santiago Becerra Gordón Gerente General	 Digitally signed by GALO SANTIAGO BECERRA GORDÓN
	Fecha de Aprobación: 19 de enero de 2026

Tabla de Contenidos / Índice

1. Datos de Identificación de la Entidad de Certificación de Información y Servicios Relacionados Acreditada..... 9

2. Introducción..... 9

2.1. Visión General..... 10

2.2. Nombre e Identificación del Documento..... 10

2.3. Participantes de la PKI..... 11

2.3.1. Autoridad de Certificación Raíz (AC Raíz)..... 11

2.3.2. Autoridad de Registro (AR)..... 11

2.3.3. Suscriptores (Titulares)..... 11

2.3.4. Partes Confiables..... 11

2.3.5. Otros Participantes..... 11

2.4. Uso de los Certificados..... 11

2.4.1. Usos Permitidos..... 11

2.4.2. Usos Prohibidos..... 13

2.5. Administración de la Política..... 13

2.5.1 Organización que administra el documento..... 13

2.5.2 Persona de contacto..... 13

2.5.3 Persona que determina la idoneidad de la DPC para la política..... 14

2.5.4 Procedimientos de aprobación del CPS..... 14

2.6. Definiciones y Acrónimos..... 14

3. Publicación y Responsabilidades del Repositorio..... 17

3.1. Repositorios..... 17

3.2. Publicación de Información de Certificación..... 17

3.3. Tiempo o Frecuencia de Publicación..... 17

3.4. Control de acceso a los repositorios..... 18

4. Identificación y Autenticación..... 18

4.1. Nombres..... 18

4.1.1 Tipos de Nombres..... 18

4.1.2 Necesidad de que los nombres sean significativos..... 19

4.1.3 Anonimato o seudónimos de los suscriptores..... 19

4.1.4 Reglas para interpretar varios formatos de nombres..... 19

4.1.5 Unicidad de los nombres..... 20

4.1.6 Reconocimiento, autenticación y función de las marcas comerciales..... 20

4.2. Validación de Identidad Inicial..... 20

4.2.1. Método para probar la posesión de la clave privada..... 20

4.2.2. Autenticación de la Identidad de la organización..... 21
4.2.3. Autenticación de la Identidad individual.....21
4.2.4. Información del Suscriptor No Verificada..... 22
4.2.5. Validación de Autoridad.....22
4.2.6. Criterios de Interoperabilidad.....22
4.3. Identificación y Autenticación para Solicitudes de Re-generación de Claves (Re-key)..... 22
4.3.1. Identificación y Autenticación para Re-Key de Rutina..... 23
4.3.2. Identificación y Autenticación para Re-Key Después de Revocación..... 23
4.4 Identificación y Autenticación para Solicitudes de Revocación.....24
5. Requisitos Operativos del Ciclo de Vida del Certificado.....24
5.1. Solicitud de Certificado.....24
5.1.1. Quién puede enviar una solicitud de certificado..... 24
5.1.2. Proceso de Inscripción y responsabilidades.....25
5.2. Procesamiento de Solicitudes de Certificado..... 25
5.2.1. Realización de Funciones de Identificación y Autenticación.....26
5.2.2. Aprobación o rechazo de solicitudes de certificado..... 26
5.2.3. Tiempo para procesar solicitudes de certificado..... 27
5.3. Emisión de Certificado.....27
5.3.1. Acciones de la AC durante la emisión..... 27
5.3.2. Notificaciones al Suscriptor por parte de la CA sobre la Emisión del Certificado..... 27
5.4. Aceptación del Certificado.....27
5.4.1. Conducta que constituye la aceptación del certificado..... 28
5.4.2. Publicación del Certificado por la AC..... 28
5.4.3. Notificación de la Emisión del Certificado por parte de la AC a otras entidades..... 28
5.5. Uso de Pares de Claves y Certificados..... 28
5.5.1. Uso del Certificado y Clave Privada del Suscriptor.....28
5.5.2. Uso de la clave pública y del certificado por parte de los terceros confiantes..... 29
5.6. Renovación de Certificados..... 30
5.6.1. Circunstancias para la renovación de un certificado.....30
5.6.2. Quién puede solicitar la Renovación.....30
5.6.3. Procesamiento de Solicitudes de Renovación de Certificados.....30
5.6.4. Notificación de la emisión de un nuevo certificado al suscriptor..... 30
5.6.5. Conducta que constituye aceptación de un certificado de renovación..... 30
5.6.6. Publicación del certificado renovado por la AC..... 30
5.6.7 Notificación de la emisión del certificado por la AC a otras entidades.....30
5.7. Regeneración de Claves (Re-key).....30
5.7.1. Circunstancias para la Renovación de la Clave del Certificado.....30
5.7.2. Quién puede Solicitar la Certificación de una Nueva Clave Pública.....30

5.7.3. Procesamiento de Solicitudes de Renovación de Claves de Certificado..... 31
5.7.4. Notificación de la Emisión de un Nuevo Certificado al Titular..... 31
5.7.5. Conducta que Constituye Aceptación de un Certificado con Nueva Clave..... 31
5.7.6. Publicación del Certificado Renovado en la AC..... 31
5.8. Modificación de Certificado..... 31
5.8.1. Circunstancias para la Modificación del Certificado..... 31
5.8.2. Quién puede solicitar la Modificación del Certificado..... 31
5.8.3. Procesamiento de Solicitudes de Modificación del Certificado..... 31
5.8.4. Notificación de la Emisión de un Nuevo Certificado al Titular..... 31
5.8.5. Conducta que constituye aceptación de un certificado modificado..... 32
5.8.6. Publicación del certificado modificado por la CA..... 32
5.8.7. Notificación de la emisión del certificado por la AC a otras entidades..... 32
5.9. Revocación y Suspensión de Certificados..... 32
5.9.1. Circunstancias para la Revocación..... 32
5.9.2. Quién puede solicitar la Revocación..... 33
5.9.3. Procedimiento para la solicitud de Revocación..... 33
5.9.4. Plazo de gracia para la Solicitud de Revocación..... 34
5.9.5. Tiempo dentro del cual la AC debe procesar la solicitud de revocación..... 34
5.9.6. Requisito de verificación de revocación para las partes confiantes..... 35
5.9.7. Frecuencia de Emisión de CRL..... 35
5.9.8. Latencia máxima de la CRL..... 35
5.9.9. Disponibilidad de Comprobación de estado/revocación en Línea..... 35
5.9.10. Requisitos de Comprobación de Revocación en Línea..... 35
5.9.11. Otras formas de Anuncios de Revocación Disponibles..... 36
5.9.12. Requisitos especiales en caso de compromiso de clave privada..... 36
5.9.13 Circunstancias para la Suspensión..... 36
5.9.14. Quién puede solicitar la Suspensión..... 36
5.9.15. Procedimiento para solicitud de Suspensión..... 36
5.9.16. Límite de Tiempo para la Suspensión..... 36
5.10. Servicios de Estatus de Certificados..... 37
5.10.1 Características Operativas..... 37
5.10.2. Disponibilidad del Servicio..... 37
5.10.3. Características Opcionales..... 37
5.11. Fin de la Suscripción..... 37
5.12. Custodia y Recuperación de Claves..... 37
5.12.1 Política y prácticas de Depósito y Recuperación de Llaves..... 38
5.12.2 Política y Prácticas de Encapsulamiento y Recuperación de Llaves de Sesión..... 38
6. Controles Gestión, Operativos y Físicos..... 38

6.1. Controles de Seguridad Física....38
6.1.1. Localización del Sitio y Construcción....38
6.1.2. Acceso Físico....38
6.1.3. Energía y Aire Acondicionado....39
6.1.4. Exposición al Agua....39
6.1.5. Prevención y Protección contra Incendios....39
6.1.6. Almacenamiento de Medios....39
6.1.7. Eliminación de Residuos....39
6.1.8. Copias de Seguridad fuera del Sitio....39
6.2. Controles de Procedimientos....40
6.2.1. Roles de Confianza....40
6.2.2. Número de personas requeridas para una tarea....40
6.2.3. Identificación y Autenticación de cada Rol....40
6.2.4. Roles que requieren separación de funciones....41
6.3. Controles de Seguridad del Personal....42
6.3.1. Requisitos de calificaciones, experiencia y autorizaciones....42
6.3.2. Procedimientos de verificación de antecedentes....42
6.3.3. Requisitos de capacitación....42
6.3.4. Frecuencia y requisitos de actualización de la formación....43
6.3.5. Frecuencia y secuencia de Rotación de Personal....43
6.3.6. Sanciones por acciones no autorizadas....43
6.3.7. Requisitos para contratistas independientes....43
6.3.8. Documentación suministrada al personal....44
6.4. Procedimientos de Registro de Auditorías....44
6.4.1. Tipos de Eventos Registrados....44
6.4.2. Frecuencia de Procesamiento de Registros....45
6.4.3. Período de Retención de Registros de Auditoría....45
6.4.4. Protección de los Registros de Auditoría....45
6.4.5. Procedimientos de Respaldo de Registros de Auditoría....45
6.4.6. Sistema de Recolección de Registros de Auditoría (interno vs. externo)....45
6.4.7. Notificación al sujeto causante del evento....46
6.4.8. Evaluaciones de Vulnerabilidad....46
6.5. Archivo de Registros....46
6.5.1. Tipos de Registros Archivados....46
6.5.2. Periodo de Retención para Archivo....46
6.5.3 Protección del Archivo....46
6.5.4. Procedimientos de Respaldo del Archivo....47
6.5.5. Requisitos para Sellado de Tiempo de Registros....47

6.5.6. Sistema de Recopilación de Archivos (interno o externo)....47
6.5.7. Procedimientos para obtener y verificar información de archivo....47
6.6. Cambio de Claves....47
6.7. Compromiso y Recuperación ante Desastres....47
6.7.1. Procedimientos de manejo de incidentes y compromisos....47
6.7.2. Recursos informáticos, software y/o datos corruptos....48
6.7.3. Procedimientos de recuperación ante el compromiso clave privada de la entidad....48
6.7.4. Capacidades de continuidad comercial después de un desastre....48
6.8. Terminación de una AC o AR....49
7. Controles Técnicos de Seguridad....49
7.1. Generación de par de Llaves e Instalación....49
7.1.1. Generación de par de Llaves....49
7.1.2. Entrega de Clave Privada al Suscriptor....49
7.1.3. Entrega de Clave Pública al Emisor del Certificado....49
7.1.4. Entrega de clave pública de AC a Terceros que Confían....50
7.1.5. Tamaños de Claves....50
7.1.6. Generación de Parámetros de Clave Pública y Control de Calidad....50
7.1.7. Propósitos de Uso de Claves (según X.509 v3. Campo de uso de claves)....50
7.2. Protección de Clave Privada y Controles de Ingeniería del Módulo Criptográfico....50
7.2.1. Estándares y controles del Módulo Criptográfico....50
7.2.2. Control multipersona de la Llave Privada (n de m)....51
7.2.3. Custodia de Clave Privada....51
7.2.4. Copia de Seguridad de Clave Privada....51
7.2.5. Archivo de Clave Privada....51
7.2.6. Transferencia de Clave Privada hacia o desde un Módulo Criptográfico....51
7.2.7. Almacenamiento de Clave Privada en Módulo Criptográfico....51
7.2.8. Método de Activación de Clave Privada....51
7.2.9. Método de Desactivación de Clave Privada....51
7.2.10. Método de Destrucción de Clave Privada....52
7.2.11. Clasificación del Módulo Criptográfico....52
7.3. Otros Aspectos de la Gestión de pares de Claves....52
7.3.1. Archivo de la Clave Pública....52
7.3.2. Periodos operativos de certificado y períodos de uso de pares de claves....52
7.4. Datos de Activación....52
7.4.1. Generación e Instalación de Datos de Activación....52
7.4.2. Protección de Datos de Activación....52
7.4.3. Otros Aspectos de los Datos de Activación....53
7.5. Controles de Seguridad Informática....53

7.5.1 Requisitos Técnicos específicos de Seguridad Informática....53
7.5.2. Clasificación de Seguridad Informática....53
7.6. Controles Técnicos del Ciclo de Vida....53
7.6.1. Controles de Sistema de Desarrollo....53
7.6.2. Controles de Gestión de Seguridad....54
7.6.3. Controles de Seguridad de Ciclo de Vida....54
7.7. Controles de Seguridad de Red....54
7.8. Sellado de Tiempo....54
8. Perfiles de Certificados, CRL y OCSP....55
8.1. Perfil del Certificado....55
8.1.1. Número de Versión....55
8.1.2. Extensiones de los certificados....56
8.1.3. Identificación de Objeto del Algoritmo....56
8.1.4. Formas de los Nombres....56
8.1.5. Restricciones de nombres....56
8.1.6. Identificador de objeto de la política de certificados....56
8.1.7. Uso de la extensión de Restricciones de Políticas....57
8.1.8. Sintaxis y semántica de calificadores de política....57
8.1.9. Semántica de procesamiento para la extensión crítica de Política de Certificados....57
8.2. Perfil CRL....57
8.2.1. Número de versión....57
8.2.2. Extensiones de CRL....57
8.3. Perfil OCSP....58
8.3.1. Número de versión....58
8.3.2. Extensiones OCSP....58
9. Auditorías de Cumplimiento y Otras Evaluaciones....58
9.1. Frecuencia y Circunstancia de la evaluación....58
9.2. Identidad y Calificaciones del Evaluador....58
9.3. Relación del Evaluador con la Entidad Evaluada....58
9.4. Temas cubiertos en la Evaluación....58
9.5. Acciones a tomar como Resultado de Deficiencias....59
9.6. Comunicación de resultados....59
10. Otros Asuntos Comerciales y Legales....59
10.1. Tarifas....59
10.1.1 Tarifas de Emisión o Renovación de Certificados....59
10.1.2. Tarifas de Acceso a Certificados....60
10.1.3. Tarifas de Acceso a Información de Revocación y Estatus....60
10.1.4. Tarifas para Otros Servicios....60

10.1.5. Políticas de reembolso.....60
10.2. Responsabilidad Financiera.....60
10.2.1. Cobertura de Seguros.....60
10.2.2. Otros activos.....61
10.2.3. Cobertura de seguro o garantía para las entidades finales.....61
10.3. Confidencialidad de la Información Empresarial.....61
10.3.1. Alcance de la Confidencialidad de Información.....61
10.3.2. Información No Confidencial.....61
10.3.3. Responsabilidad de Proteger la Información Confidencial.....61
10.4. Privacidad de la Información Personal.....62
10.4.1. Plan de Privacidad.....62
10.4.2. Información que se trata como Privada.....62
10.4.3. Información no privada.....62
10.4.4. Responsabilidad para proteger información privada.....62
10.4.5. Aviso y Consentimiento de Uso de Información Privada.....62
10.4.6. Divulgación de Conformidad con Procesos Judiciales o Administrativos.....62
10.4.7. Otras circunstancias de divulgación de información.....62
Ninguna otra fuera de las legales.....62
10.5. Derechos de Propiedad Intelectual.....63
10.6. Representaciones y Garantías.....63
10.6.1. Representaciones y Garantías de la AC.....63
10.6.2. Representaciones y Garantías de la AR.....64
10.6.3. Representaciones y Garantías del Suscriptor.....64
10.6.4. Representaciones y Garantías de los Terceros que Confían.....66
10.6.5. Representaciones y Garantías de Otros Participantes.....66
10.7. Exclusión de Garantías.....67
10.8. Limitación de Responsabilidad.....67
10.9. Indemnizaciones.....67
10.10. Vigencia y Terminación.....68
10.10.1. Plazo.....68
10.10.2. Terminación.....68
10.10.3. Efectos de la Terminación y supervivencia.....68
10.11. Notificaciones y Comunicaciones Individuales con los Participantes.....69
10.12. Enmiendas.....69
10.12.1. Procedimiento para Enmiendas.....69
10.12.2. Mecanismos de Notificación y Período.....69
10.12.3 Circunstancias en las que debe cambiar el OID.....69
10.13. Disposiciones de Resolución de Disputas.....69

10.14. Ley Aplicable....70
10.15. Cumplimiento de la Ley Aplicable.... 70
10.16. Disposiciones varias....70
10.16.1. Acuerdo Completo.... 70
10.16.2. Cesión.... 70
10.16.3. Divisibilidad....71
10.16.4. Ejecución....71
10.16.5. Fuerza Mayor.... 71
10.17. Otras Disposiciones.... 71
11. Control de Cambios.... 71

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DICERT (DPC)

1. Datos de Identificación de la Entidad de Certificación de Información y Servicios Relacionados Acreditada[1]

Mediante Resolución ARCOTEL _____ del _____, la Agencia de Regulación y Control de las Telecomunicaciones emitió el Título Habilitante: Acreditación como una Entidad de Certificación de Información y Servicios Relacionados (ECI), mediante el cual otorga la Acreditación como Entidad de Certificación de Información y Servicios Relacionados a favor de la compañía **DICERT DISTRIBUIDORA INTERNACIONAL DE CERTIFICACION ELECTRONICA S.A.,** empresa constituida bajo las leyes de la República del Ecuador, con domicilio en la ciudad de Quito, identificada con su nombre comercial **DICERT**.

Sus **datos de Identificación** son los siguientes:

DICERT DISTRIBUIDORA INTERNACIONAL DE CERTIFICACION ELECTRONICA S.A.
Correo electrónico: soporte@dicert.com.ec
Dirección: Av. Ulpiano Becerra N2-242 y Panamericana Norte. Quito, Ecuador
Número de teléfono: +593 992987687
Código postal: EC170201
Sitio web: www.dicert.com.ec

Persona de Contacto:
Correo electrónico: galo@dicert.com.ec
Dirección: Av. Ulpiano Becerra N2-242 y Panamericana Norte. Quito, Ecuador
Número de teléfono: +593 992987687
Código postal: EC170201
Sitio web: www.dicert.com.ec

2. Introducción[2]

La presente **Declaración de Prácticas de Certificación (DPC)** establece las disposiciones y procedimientos aplicables a la Infraestructura de Clave Pública (PKI) de DICERT. Este documento

[1] Atiende a la norma técnica ARCOTEL-2024-0176: Art. 5, Numeral 1, a)
[2] Atiende a la Sección 4.1 de la RFC 3647 y norma técnica ARCOTEL-2024-0176: Art. 5, Numeral 1, i)

detalla las políticas, roles, responsabilidades, procesos y controles implementados por DICERT para garantizar la emisión y gestión segura de certificados digitales, alineados con las mejores prácticas internacionales y la norma RFC 3647.

La DPC está dirigida a todos los participantes de la PKI, incluyendo autoridades de certificación (ACs), autoridades de registro (ARs), suscriptores, partes confiables y otros terceros relacionados, definiendo los requisitos operativos y las responsabilidades de cada una de estas entidades en el ciclo de vida de los certificados emitidos por DICERT.

2.1. Visión General[3]

La Infraestructura de Clave Pública (PKI) de DICERT ofrece un conjunto integral de servicios de certificación de información, diseñados para garantizar la seguridad, integridad, autenticidad y no repudio de las transacciones electrónicas. Entre los servicios más destacados se incluyen la emisión de **certificados de firma electrónica** para personas naturales, representantes legales y miembros de empresa o en relación de dependencia, así como **certificados de sello electrónico** para entidades públicas y privadas. También proporciona servicios especializados como **sellados de tiempo, declaraciones electrónicas de atributos, conservación y almacenamiento seguro de mensajes de datos, y la entrega electrónica certificada**. Estos servicios están respaldados por una infraestructura confiable y segura, que garantiza la protección contra alteraciones y la disponibilidad de los datos en todo momento.

Además, DICERT opera servicios de gestión avanzada de certificados, como la publicación de listas de certificados revocados (CRLs) y la consulta en línea del estado de certificados (OCSP), permitiendo a las partes confiables verificar en tiempo real la validez de los certificados emitidos.

2.2. Nombre e Identificación del Documento[4]

Nombre del Documento: Declaración de Prácticas de Certificación DICERT (DPC).

Identificador del Documento (OID): 1.3.6.1.4.1.62486.1

Versión del documento: Versión 2.0, publicada el 19 de enero de 2026.

Este documento describe las prácticas implementadas por DICERT en su rol como Autoridad de Certificación (**AC**) dentro de su PKI.

[3] Atiende a la Sección 4.1.1 de la RFC 3647
[4] Atiende a la Sección 4.1.2 de la RFC 3647 y norma técnica ARCOTEL-2024-0176: Art. 5, Numeral 1, b)

2.3. Participantes de la PKI[5]

La Infraestructura de Clave Pública (**PKI**) de DICERT está compuesta por múltiples entidades y participantes que desempeñan roles clave en la gestión, emisión, validación y uso de certificados digitales. A continuación, se describen los principales participantes de la PKI:

2.3.1. Autoridad de Certificación Raíz (AC Raíz)

Incluye la AC Raíz (máximo punto de confianza, emite certificados para AC Intermedias) y la AC Intermedia (emite certificados a suscriptores finales).

2.3.2. Autoridad de Registro (AR)

Intermediario responsable de la identificación, verificación y validación de datos de los solicitantes antes de remitir la aprobación a la AC.

2.3.3. Suscriptores (Titulares)

Personas naturales, representantes legales o personas jurídicas a quienes se emiten los certificados.

Los suscriptores son responsables del uso adecuado de sus certificados, así como de la custodia de sus claves privadas, según lo establecido en las políticas de certificación de DICERT.

2.3.4. Partes Confiables

Entidades que confían en los certificados de DICERT para validar firmas o sellos, verificando su estado mediante CRL o OCSP.

2.3.5. Otros Participantes

Incluye a la Autoridad de Validación (AV) para servicios OCSP y CRL, y Administradores de la AC.

2.4. Uso de los Certificados[6]

Los certificados emitidos por DICERT están diseñados para garantizar la seguridad, autenticidad, integridad y no repudio de transacciones electrónicas, respaldando una amplia gama de aplicaciones tecnológicas. A continuación, se detallan los usos permitidos y las restricciones aplicables según las políticas de certificación:

2.4.1. Usos Permitidos

[5] Atiende a la Sección 4.1.3 de la RFC 3647
[6] Atiende a la Sección 4.1.4 de la RFC 3647 y norma técnica ARCOTEL-2024-0176: Art. 5, Numeral 1, g)

Los certificados emitidos por DICERT son adecuados para las siguientes aplicaciones y casos de uso:

1. **Firma Electrónica Avanzada**:
    - Certificados de personas naturales para firmar digitalmente documentos con validez legal y garantizar la identidad del firmante.
    - Certificados de representantes legales para firmar en nombre de personas jurídicas públicas o privadas y garantizar la identidad del firmante.
    - Certificados de miembros de empresa, empleados con relación de dependencia u otros cargos específicos para asegurar la autenticidad de documentos corporativos y garantizar la identidad del firmante.
2. **Sello Electrónico**:
    - Certificados de sello electrónico institucional que permiten a las entidades públicas o privadas garantizar la autenticidad de documentos y datos electrónicos, asegurando la integridad y no repudio de la información transmitida.
3. **Sellado de Tiempo:**
    - Generación de sellado de tiempo para certificar la existencia de documentos, datos o transacciones electrónicas en un momento temporal específico. Este servicio es esencial para garantizar la integridad y trazabilidad de datos en auditorías, contratos o registros legales.
4. **Entrega Electrónica Certificada**:
    - Envío de documentos o datos electrónicos entre partes confiables, proporcionando evidencia verificable de la transmisión, recepción e integridad del contenido, mediante el uso de firmas electrónicas avanzadas y sellado de tiempo.
5. **Declaraciones Electrónicas de Atributos**:
    - Certificación de atributos específicos, como por ejemplo, pero sin limitar a: roles, derechos, autorizaciones o permisos, tanto de personas naturales como jurídicas, inclusive objetos. Estas declaraciones permiten autenticar características particulares del titular ante terceros.
6. **Conservación y Almacenamiento Seguro de Mensajes de Datos**:
    - Custodia digital de documentos electrónicos con mecanismos que aseguren la integridad, confidencialidad y trazabilidad, respaldados por certificados que garantizan la validez y el historial de los datos almacenados.
7. **Servicios de Validación**:
    - Validación de certificados mediante CRLs (Listas de Certificados Revocados) y el protocolo OCSP (Online Certificate Status Protocol), garantizando el estado de validez de los certificados en tiempo real.
8. **Seguridad en Comunicaciones Electrónicas**:
    - Cifrado de datos y autenticación de servidores mediante certificados de infraestructura segura (TLS/SSL).

2.4.2. Usos Prohibidos[7]

DICERT establece las siguientes **restricciones** en el uso de los certificados emitidos, con el objetivo de evitar actividades que comprometan la seguridad, confiabilidad o cumplimiento legal:

1. **Usos Ilícitos**:
    - Actividades que violen normativas legales locales, nacionales o internacionales, tales como fraude, suplantación de identidad o cibercrimen.
2. **Aplicaciones no autorizadas**:
    - Uso de certificados para fines no contemplados en los términos y condiciones del servicio, como firmar o autenticar actividades fuera del alcance definido en las políticas de certificación.
3. **Aplicaciones Críticas no Autorizadas**:
    - Certificados utilizados en sistemas críticos que puedan poner en riesgo la seguridad pública, la infraestructura nacional o servicios esenciales.
4. **Modificación de Documentos Sellados o Firmados**:
    - Alteración no autorizada de documentos electrónicos previamente firmados o sellados, lo que comprometería la integridad de las transacciones.
5. **Cualquier otro uso no especificado**:
    - Los certificados no podrán ser empleados en ningún uso que no haya sido específicamente permitido en la Declaración de Prácticas de Certificación (DPC) de DICERT.

2.5. Administración de la Política[8]

2.5.1 Organización que administra el documento

La responsabilidad de la redacción, administración, mantenimiento y actualización de esta Declaración de Prácticas de Certificación (DPC) recae exclusivamente sobre **DICERT DISTRIBUIDORA INTERNACIONAL DE CERTIFICACIÓN ELECTRÓNICA S.A.** La entidad garantiza que este documento se mantenga alineado con los cambios tecnológicos y las disposiciones legales vigentes en el Ecuador.

2.5.2 Persona de contacto

Para cualquier consulta, aclaración o notificación relacionada con la aplicación de las prácticas descritas en este documento, los interesados pueden dirigirse a:

- **Atención:** Galo Santiago Becerra Gordón (Gerente General).
- **Dirección:** Av. Ulpiano Becerra N2-242 y Panamericana Norte. Quito, Ecuador.

[7] Atiende a la Sección 4.1.4 de la RFC 3647
[8] Atiende a la Sección 4.1.5 y 6 de la RFC 3647 y norma técnica ARCOTEL-2024-0176: Art. 5, Numeral 1, h)

- **Correo electrónico:** soporte@dicert.com.ec / galo@dicert.com.ec.
- **Teléfono:** +593 992987687
- **Sitio web:** www.dicert.com.ec

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

La Gerencia General de DICERT actúa como la autoridad competente para determinar que las prácticas operativas descritas en esta DPC son idóneas y suficientes para dar cumplimiento a las Políticas de Certificación (PC) de la entidad. Esta determinación se basa en análisis periódicos de cumplimiento técnico y legal frente a la normativa de ARCOTEL y los estándares internacionales.

2.5.4 Procedimientos de aprobación del CPS

La entrada en vigencia de esta DPC, así como de cualquier modificación sustancial o actualización de versión, requiere la aprobación formal y expresa del **Gerente General de DICERT**. El procedimiento de aprobación incluye:

1. **Revisión Técnica:** Verificación de la consistencia de los controles de seguridad y procesos operativos.
2. **Validación Jurídica:** Aseguramiento del cumplimiento con la Ley de Comercio Electrónico y Normas Técnicas de ARCOTEL.
3. **Firma y Fecha:** El documento se considera aprobado tras la inserción de la firma del Gerente General y la indicación de la fecha de emisión.
4. **Notificación:** Toda versión aprobada debe ser comunicada a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) para su registro y control conforme a la ley.

2.6. Definiciones y Acrónimos[9]

Los términos utilizados en este documento se entienden según lo especificado a continuación:

Solicitante: Persona natural o representante legal que solicita (o busca renovar) un certificado. El solicitante puede volverse *suscriptor* una vez que el certificado sea emitido. El solicitante puede solicitar un certificado para sí mismo o en estado de representante legal de una empresa registrada con RUC.

[9] Atiende a la Sección 4.1.6 de la RFC 3647

Reporte de auditoría: Es un reporte de un Auditor Calificado que expresa el cumplimiento de controles y procesos de una entidad de certificación.

Infraestructura de Llave Pública: Es el conjunto de personas, políticas, procedimientos y sistemas informáticos necesarios para proporcionar servicios de autenticación, cifrado, integridad y no repudio, mediante el uso de criptografía de llaves públicas y privadas, y de certificados electrónicos.

Certificado: Es un mensaje de datos firmado electrónicamente por un prestador de servicios de certificación, el cual vincula la llave pública a un firmante y confirma su identidad.

Llave pública: Es parte del par de llaves definido en la infraestructura PKI, la cual puede ser públicamente compartida por el propietario de la correspondiente Llave Privada y que es utilizada por una Entidad de Confianza para verificar la firma digital creada con la Llave Privada.

Llave privada: Es parte del par de llaves definido en la infraestructura PKI, la cual es almacenada de forma segura por el propietario del par de llaves. Se utiliza para crear firmas digitales de documentos o mensajes.

Sistema de Gestión de Certificados: Es el sistema que utiliza DICERT para el proceso, aprobación, emisión, consulta y almacenamiento de certificados. Incluye una base de datos, sistemas operativos e infraestructura de la nube.

Sistema de Emisión de Certificados: Es el sistema que firma los certificados.

Entidad o persona jurídica: Es una asociación, corporación, sociedad, fideicomiso, entidad de gobierno u otra entidad registrada legalmente en un país.

Prestador de Servicios de Certificación: Es la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con certificados electrónicos.

Titular: Persona, entidad o componente informático para el cual se expide un certificado electrónico y es aceptado por éste o por su responsable.

Parte confiable: Es la entidad que confía en la información contenida en el certificado.

Acuerdo de entidad de confianza: Es un acuerdo entre DICERT y una parte confiable que debe ser leída y aceptada antes de validar, confiar o usar un certificado y está disponible para referencia mediante solicitud.

Declaración de voluntad: Es un acuerdo que debe ser leído y aceptado por un solicitante antes de aplicar por un certificado. La declaración de voluntad es específica para el certificado digital y se presenta durante el proceso en línea de solicitud de un certificado.

X.509: Es el estándar para certificados y su correspondiente framework de autenticación.

Los acrónimos y abreviaciones que se usan a lo largo de este documento se definen a continuación:

AC: Autoridad de Certificación.
AR: Autoridad de Registro.
AV: Autoridad de Validación.
CRL: Lista de Revocación de Certificados (Certificate Revocation List).
CN: Nombre Común (Common Name) . Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
CSR: Solicitud de Firma de Certificado (Certificate Signing Request). Conjunto de datos que contienen una llave pública y su firma electrónica utilizando la llave privada asociada. Es enviada a la Autoridad de Certificación para la emisión de un certificado digital que contenga dicha llave pública.
DN: Nombre Distintivo (Distinguished Name). Identificación unívoca de una entrada dentro de la estructura de directorio X.500.
HSM: Módulo de seguridad criptográfico utilizado para almacenar llaves y realizar operaciones criptográficas de modo seguro (Hardware Security Module).
IEFT: Organismo de estandarización de Internet (Internet Engineering Task Force).
O: Organización. Atributo del DN dentro de la estructura de directorio X.500.
OSCP: Protocolo de Estado de Certificados en Línea (Online Certificate Status Protocol). Este protocolo permite comprobar en línea la vigencia de un certificado digital.
OID: Identificador de objeto único (Object Identifier).
OU: Atributo del DN dentro de la estructura de directorio X.500 (Organizational Unit).
PC: Política de Certificación.
PKI: Infraestructura de Llave Pública (Public Key Infrastructure).
RFC: Solicitud de Comentarios (Request For Comments). Estándar emitido por la IEFT.
RSA: Rivest Shamir Adleman.
SHA: Algoritmo de Hash Seguro (Secure Hash Algorithm).
SSL: Capa de Conexión Segura (Secure Socket Layer).
TLS: Seguridad de la Capa de Transporte (Transport Layer Security).
TSA: Autoridad de Sellado de Tiempo (Time Stamping Authority).
URL: Localizador Uniforme de Recursos (Uniform Resource Locator).

3. Publicación y Responsabilidades del Repositorio[10]

3.1. Repositorios

DICERT opera directamente los repositorios que soportan su Infraestructura de Clave Pública (**PKI**). Estos repositorios están diseñados para garantizar la disponibilidad, integridad y seguridad de la información publicada, proporcionando un punto central de acceso para las partes interesadas, incluyendo suscriptores, partes confiables y otras entidades involucradas en la PKI.

3.2. Publicación de Información de Certificación

Los repositorios administrados por DICERT ponen a disposición del público la siguiente información relacionada con la PKI:

1. **Documentación Operativa:** Tales como Políticas de Certificación (PC), Declaración de Prácticas de Certificación (DPC), y toda información relevante sobre los servicios para dar a conocer al público.
2. **Listas de Certificados Revocados (CRLs)**: Listas actualizadas que contienen los certificados revocados, incluyendo los motivos y fechas de revocación.
3. **Estado de los Certificados**: Información sobre la validez de los certificados, disponible mediante mecanismos como el Protocolo de Estado de Certificados en Línea (**OCSP**).

3.3. Tiempo o Frecuencia de Publicación[11]

DICERT garantiza que la información publicada en sus repositorios esté siempre actualizada, siguiendo los siguientes plazos:

1. **Estado de certificados emitidos (OCSP):**
    - La información sobre el estado de los certificados está disponible en tiempo real (inmediatamente) mediante el protocolo OCSP, permitiendo validaciones instantáneas.
2. **Listas de Certificados Revocados y Suspendidos (CRLs)**:
    - Se generan y publican cada 24 horas, garantizando la actualización continua de los datos sobre certificados revocados y suspendidos.
    - En casos excepcionales, como revocaciones críticas, DICERT emite CRLs de emergencia antes del vencimiento de la lista actual.
    - Cada CRL está identificada con un número secuencial único que asegura su autenticidad y rastreo.

[10] Atiende a la Sección 4.2 y 6 de la RFC 3647 y norma técnica ARCOTEL-2024-0176: Art. 5, Numeral 1, j)
[11] Atiende a la Sección 4.2 de la RFC 3647 y norma técnica ARCOTEL-2024-0176: Art. 5, Numeral 1, j), 2)

- Las CRLs se almacenan durante un período de 10 años para fines de auditoría y cumplimiento normativo.

3. **Documentación Operativa**:
   - Se publican y actualizan inmediatamente siempre que haya cambios relevantes en las políticas o prácticas de certificación.

3.4. Control de acceso a los repositorios

El Repositorio está disponible públicamente. DICERT, en conjunto con sus Proveedores de Servicios, operan los controles de seguridad física y lógica para proteger el repositorio de modificación o eliminación no autorizada.

4. Identificación y Autenticación[12]

4.1. Nombres

En la PKI de DICERT, los nombres asignados a los sujetos en los certificados digitales siguen estrictamente los estándares internacionales establecidos y la norma técnica ARCOTEL-2024-0176, garantizando que los datos sean representativos, únicos y significativos. A continuación, se describen los atributos que conforman el campo *Subject* del certificado digital:

4.1.1 Tipos de Nombres

Los certificados emitidos por DICERT utilizan nombres distinguidos (**Distinguished Names - DN**) conformes al estándar X.501. Los atributos comunes incluyen:

Atributo	Descripción
Country Name (C)	País donde reside el titular de la firma
Locality Name (L)	Localidad o ciudad del titular de la firma
Organization Name (O)	Se especificará el nombre de la Persona Natural o Persona Jurídica (Pública o Privada) a la que pertenece el Signatario o con quien tiene relación de dependencia.
Organizational Unit Name (OU)	Se especificará el Departamento o Área al que pertenece el Signatario o el tipo de vinculación con la Persona Natural o Persona Jurídica (Pública o

[12] Atiende a la Sección 4.3 y 6 de la RFC 3647 y norma técnica ARCOTEL-2024-0176: Art. 5, Numeral 1, k)

	Privada) que tiene relación de dependencia. // Nombre de la Unidad Organizativa de la Persona Jurídica (Pública o Privada).
Title	Título o especialidad del titular de la firma.
Surname	Apellidos del titular de la firma, como constan en el documento oficial de identificación.
Given Name	Nombres del titular de la firma, como constan en el documento oficial de identificación.
Serial Number	Número del documento oficial de identificación del titular, codificado según ETSI EN 319 412-1.
Organization Identifier	Número de Registro Único de Contribuyente (RUC) de la organización, si corresponde, codificación acorde la ETSI EN 319 412-1.
Common Name (CN)	Nombres y apellidos completos del titular de la firma.

4.1.2 Necesidad de que los nombres sean significativos[13]

Los nombres asignados deben ser significativos y representar explícitamente al titular de la firma, ya sea una persona natural, un representante legal o una persona jurídica.

Los nombres deben ser únicos dentro de la PKI de DICERT. Esto se garantiza mediante la combinación de atributos, como el **Serial Number** y el **Common Name (CN)**, que permiten identificar de manera inequívoca a cada titular.

4.1.3 Anonimato o seudónimos de los suscriptores

No se permite. De acuerdo con la Ley de Comercio Electrónico de Ecuador, los certificados deben identificar plenamente al titular. DICERT no emite certificados anónimos ni bajo seudónimos.

Se podrán emitir certificados con el uso de pseudónimos en los casos de declaraciones electrónicas de atributos, siendo el sistema de DICERT quien asigna un identificador único aleatorio en el Serial Number, de esta manera se mantiene el control de la autenticidad y se logra la trazabilidad del titular del certificado.

4.1.4 Reglas para interpretar varios formatos de nombres

[13] Atiende a la Sección 4.3.1 y 6 de la RFC 3647

Los nombres asignados a los sujetos en los certificados digitales son interpretados de acuerdo con los estándares de codificación especificados en la normativa ETSI EN 319 412-1 y las reglas establecidas por los estándares X.509 v3 y RFC 5280.

1. **Country Name (C)**: Se utiliza el código ISO 3166 del país donde reside el titular.
2. **Common Name (CN)**: Este atributo es el nombre principal del sujeto, compuesto por los nombres y apellidos completos del titular.
3. **Serial Number**: Se utiliza para codificar el número de identificación oficial del titular, garantizando su unicidad dentro de la PKI.
4. **Organization Identifier**: Se utiliza para codificar el número de identificación oficial del titular, nombre comercial o su organización, garantizando su unicidad dentro de la PKI.

4.1.5 Unicidad de los nombres

DICERT garantiza la unicidad del DN mediante la inclusión del número de cédula o RUC del suscriptor, asegurando que no existan dos certificados con el mismo DN para distintas personas.

4.1.6 Reconocimiento, autenticación y función de las marcas comerciales

DICERT no garantiza derechos de propiedad intelectual sobre nombres incluidos en los certificados. Sin embargo, se reserva el derecho de rechazar nombres que infrinjan marcas notorias registradas.

Los Solicitantes de Certificados tienen prohibido solicitar certificados con contenido que infrinja la propiedad intelectual y derechos comerciales de terceros. Los solicitantes deben utilizar su nombre registrado en documentación oficial. En el caso de personas jurídicas, el nombre debe corresponder al registrado oficialmente en los documentos legales de la organización.

4.2. Validación de Identidad Inicial[14]

La validación de identidad inicial es un proceso crítico dentro de la PKI de DICERT, que asegura que los certificados digitales emitidos estén respaldados por identidades auténticas y verificadas, ya sean de personas naturales, representantes legales o entidades jurídicas. Este proceso incluye la verificación de la identidad del solicitante, la autenticación de la información proporcionada y la validación de la autoridad cuando se actúe en representación de una organización.

4.2.1. Método para probar la posesión de la clave privada

Antes de la emisión del certificado, el solicitante debe demostrar la posesión de la clave privada asociada a la clave pública que será registrada. Esto se realiza mediante la entrega de una **Solicitud**

[14] Atiende a la Sección 4.3.2 y 6 de la RFC 3647

de Firma de Certificado (CSR) lo cual genera un identificador único de solicitud. El proceso para la generación del CSR se define en la sección 5.2 de este documento. Esta demostración garantiza que el solicitante tiene control exclusivo sobre la clave privada vinculada al certificado.

4.2.2. Autenticación de la Identidad de la organización

Para los casos en que el solicitante sea una entidad o persona jurídica, a través de su representante legal, DICERT implementa un proceso de verificación que incluye la validación tanto de la entidad como de su representante.

1. **Documentación Requerida para la Entidad**:
    - Registro Único de Contribuyentes (RUC).
    - Estatutos, certificados o documentos legales que certifiquen la constitución de la organización o validen su existencia legal.
2. **Validación del Representante Legal en línea**:
    - Nombramiento debidamente inscrito, mandato notarial u otro documento legal que certifique que está autorizado para actuar en nombre de la organización.
    - **Presencial:** Cotejo de cédula de identidad o pasaporte original y vigente.
    - **Remota (Virtual):** Uso de biometría facial comparada contra la base de datos del Registro Civil y validación de documentos de identidad mediante algoritmos de IA.
        i. De conformidad con el artículo 17 de la Norma Técnica ARCOTEL-2024-0176, DICERT implementa mecanismos de seguridad reforzados necesarios, incluyendo al menos dos factores de autenticación independientes y seguros como los siguientes: validación biométrica, prueba de vida, biometría, para verificación de la identidad de los solicitantes de certificados en todo momento.
3. **Registro de Consentimiento**:
    - Como parte del proceso de validación inicial, el solicitante debe aceptar digitalmente los términos y condiciones del servicio, la política de privacidad, y el contrato electrónico que contiene las condiciones relacionadas con el uso y la custodia del certificado.

4.2.3. Autenticación de la Identidad individual

Para las personas naturales que soliciten un certificado digital, se realiza un proceso de autenticación basado en los siguientes pasos:

1. **Validación de la identidad**:
    - **Presencial:** Cotejo de cédula de identidad o pasaporte original y vigente.
    - **Remota (Virtual):** Uso de biometría facial comparada contra la base de datos del Registro Civil y validación de documentos de identidad mediante algoritmos de IA.

i. De conformidad con el artículo 17 de la Norma Técnica ARCOTEL-2024-0176, DICERT implementa mecanismos de seguridad reforzados necesarios, incluyendo al menos dos factores de autenticación independientes y seguros como los siguientes: validación biométrica, prueba de vida, biometría, para verificación de la identidad de los solicitantes de certificados en todo momento.

- En el caso de certificados vinculados a actividades económicas, se puede requerir el Registro Único de Contribuyentes (RUC).

2. **Registro de Consentimiento**:
   - Como parte del proceso de validación inicial, el solicitante debe aceptar digitalmente los términos y condiciones del servicio, la política de privacidad, y el contrato electrónico que contiene las condiciones relacionadas con el uso y la custodia del certificado.

4.2.4. Información del Suscriptor No Verificada

Solo se incluye información verificada. Los campos opcionales no validados (como "Cargo" si no hay respaldo) no se incluyen en el certificado.

4.2.5. Validación de Autoridad

Para validar la pertinencia de las Solicitudes de Certificados por parte del responsable de una entidad o persona jurídica, se debe verificar las facultades que dispone para el uso de un certificado electrónico, conforme a los documentos legales enviados en la Solicitud.

4.2.6. Criterios de Interoperabilidad

DICERT cumple con los perfiles de certificado definidos por ARCOTEL para asegurar la interoperabilidad con otras entidades del Estado y el sector privado.

4.3. Identificación y Autenticación para Solicitudes de Re-generación de Claves (Re-key)[15]

La re-generación de claves (**Re-key**) en la PKI de DICERT es un proceso que permite emitir un nuevo certificado digital para un titular que ya cuenta con un certificado emitido anteriormente. Este proceso garantiza la continuidad del servicio de certificación, manteniendo la seguridad y la autenticidad de la identidad del titular. A continuación, se detallan los requisitos y procedimientos aplicables para la re-generación de claves.

[15] Atiende a la Sección 4.3.3 y 6 de la RFC 3647

4.3.1. Identificación y Autenticación para Re-Key de Rutina

El Re-key rutinario se aplica cuando el certificado aún está vigente y el titular desea renovar su certificado antes de la fecha de expiración. Los requisitos de identificación y autenticación para este tipo de solicitud son los siguientes:

1. **Firma de la Solicitud con la Clave Actual**:
    - El titular debe generar una nueva clave privada y un CSR (Solicitud de Firma de Certificado), firmado con la clave privada asociada al certificado actual.
    - Este mecanismo asegura que el solicitante sea el poseedor legítimo de la clave privada asociada al certificado que está siendo renovado.
2. **Validación de Identidad**:
    - En el caso de que no haya cambios en los datos del titular (persona natural, representante legal o entidad jurídica), se reutiliza la información validada previamente, incluida la documentación y los registros de identidad del certificado original, siempre que dicha validación no supere los **24 meses** de antigüedad.
    - En caso de haber cambios en los datos del titular o la organización, se requerirá una nueva verificación de identidad, siguiendo los pasos descritos en la sección ***4.2. Validación de Identidad Inicial***.
3. **Consentimiento Digital**:
    - El solicitante debe aceptar nuevamente los términos y condiciones del servicio, así como las políticas de certificación aplicables y contrato, antes de proceder con la emisión del nuevo certificado.
4. **Aprobación Automatizada o Manual**:
    - Si la firma de la solicitud y la información enviada cumplen con los requisitos, el proceso puede completarse automáticamente.
    - En caso de inconsistencias o alertas, el proceso pasa a una revisión manual por un ejecutivo de DICERT antes de la emisión del nuevo certificado.

4.3.2. Identificación y Autenticación para Re-Key Después de Revocación

En caso de que el certificado haya sido revocado (por compromiso de clave, cese de funciones o solicitud del titular), **no se permite** un proceso abreviado de autenticación.

- **Procedimiento:** El suscriptor deberá someterse nuevamente al proceso completo de **Validación de Identidad Inicial** descrito en la sección 4.2 de esta DPC.
- **Requisito:** Se debe generar un nuevo par de claves y presentar la documentación de respaldo actualizada, eliminando cualquier presunción de validez de la identidad previa debido a la ruptura de la cadena de confianza que supuso la revocación.

4.4 Identificación y Autenticación para Solicitudes de Revocación

DICERT procesa las solicitudes de revocación previo cumplimiento de los siguientes mecanismos de autenticación para asegurar que la solicitud es legítima**:**

- **Solicitud Firmada Electrónicamente**: El titular puede enviar un formulario de revocación firmado con su propio certificado (si aún tiene acceso a la clave privada y no está comprometida).
- **Autenticación por Secreto (Passphrase)**: El uso del código de revocación único entregado al suscriptor al momento de la emisión. La provisión de este código a través de la interfaz web de DICERT se considera una autenticación válida.
- **Presencia Física o Remota**: Mediante comparecencia ante la Autoridad de Registro (AR) con su documento de identidad original o mediante el uso de biometría facial homologada en el portal de DICERT.
- **Revocación Administrativa**: En casos de orden judicial, terminación de la relación laboral (para miembros de empresa) o fallecimiento, la autenticación se realizará mediante la verificación de los documentos legales que acrediten el hecho (ej. acta de defunción, notificación legal del representante legal).

5. Requisitos Operativos del Ciclo de Vida del Certificado[16]

5.1. Solicitud de Certificado

La solicitud de certificados digitales dentro de la PKI de DICERT sigue un procedimiento estructurado y seguro, que involucra la generación del par de claves, la validación de identidad del solicitante y el procesamiento de la solicitud por parte de la Autoridad de Registro (AR) y la Autoridad de Certificación (AC). Los participantes involucrados deben cumplir con sus respectivas responsabilidades a lo largo de este proceso.

5.1.1. Quién puede enviar una solicitud de certificado

Las solicitudes de certificado pueden ser presentadas por:

- Personas naturales (individuos mayores de edad con capacidad legal).
- Mandatarios o Representantes legales de personas jurídicas.
- Empleados o miembros de empresas en relación de dependencia.

[16] Atiende a la Sección 4.4 y 6 de la RFC 3647 y la norma técnica ARCOTEL-2024-0176: Art. 5, Numeral 1, h)

- La Autoridad de Registro (AR), en representación de los solicitantes, tras validar su identidad y documentación.
- La propia AC, en casos de certificados internos o técnicos.

DICERT mantiene una lista de todos los Certificados revocados y/o rechazados anteriormente, para verificar que quien esté haciendo la Solicitud, no se encuentre en esas listas.

El Solicitante debe tener conexión a internet, un explorador de Internet y tener o crear credenciales de acceso en DICERT.

5.1.2. Proceso de Inscripción y responsabilidades

Para solicitar un Certificado, el Solicitante debe enviar a DICERT un formulario de aplicación, incluyendo una solicitud de certificado, los documentos adjuntos requeridos y cualquier otro requisito por parte de DICERT al momento de la solicitud.

La información personal de los Suscriptores es tratada conforme a las políticas de privacidad de DICERT la cual, como mínimo, establece los procedimientos y prácticas para garantizar la confidencialidad y seguridad de la información personal.

Los suscriptores garantizan que toda la información provista y contenida en el Certificado es veraz, completa, auténtica y actualizada. Además, son responsables del resguardo de su clave privada. Deben aceptar la declaración de voluntad y los términos de servicio antes de enviar la solicitud.

5.2. Procesamiento de Solicitudes de Certificado

El procesamiento de solicitudes de certificado en la PKI de DICERT se desarrolla en varias etapas controladas, que garantizan la verificación exhaustiva de la identidad del solicitante, la validez de la información suministrada, y la decisión fundamentada sobre la emisión o rechazo del certificado digital.

El procedimiento incluye:

- Verificar que el Solicitante está permitido a obtener un Certificado bajo las normas de esta DPC.
- Verificar que el Solicitante haya provisto una Solicitud de Certificados (CSR) válida y bien formada, y que contenga una firma electrónica válida.
- Obtener o generar la Llave Pública del Solicitante.
- Se capturará la aceptación digital de la aceptación de términos y condiciones, política de privacidad, política de certificación y declaración de prácticas de certificación, aceptación de tratamiento de datos personales y del contrato de prestación de servicios.

5.2.1. Realización de Funciones de Identificación y Autenticación

a. Recepción de la solicitud (CSR):

- El usuario debe ingresar a la plataforma de DICERT, crear un usuario o iniciar sesión.
- En el portal del cliente ingresar a la opción generar certificado y seleccionar el tipo de certificado a solicitar.
- Según el caso de uso, a través de un formulario dinámico, se requerirá información personal de identificación, contactabilidad y representación, así como la carga de anexos.
- El usuario deberá generar una contraseña privada para asociarla al certificado a ser emitido, cumpliendo con la política de contraseñas de DICERT.

b. Identificación y autenticación del solicitante: La AR verifica la identidad del solicitante conforme a los procedimientos definidos en la ***sección 4.2*** de esta DPC.

c. Verificación del Contenido CSR: Se evalúa que los atributos incluidos en el CSR sean coherentes con la documentación presentada, y que los campos como el Common Name, el Número de Identificación y otros, estén correctamente formateados y autorizados.

d. Evaluación de Políticas Aplicables: Se revisa que la solicitud esté alineada con la política de certificación correspondiente (por ejemplo, certificado de persona natural, representante legal, sello electrónico, etc.) y que no existan restricciones legales o contractuales que impidan su emisión.

5.2.2. Aprobación o rechazo de solicitudes de certificado

Aprobación: Si todos los datos son válidos y la solicitud cumple con las políticas técnicas y legales de DICERT, la AR aprueba la solicitud y la envía firmada a la AC, quien procederá con la emisión del certificado.

En caso que el proceso de validación automatizada genere una alerta, el proceso pasará a un estado de verificación manual, donde un ejecutivo de DICERT realizará la validación y aprobará o rechazará la emisión.

Rechazo: DICERT puede rechazar la solicitud en cualquiera de los siguientes casos:

- Datos falsos, incompletos o inconsistentes.
- Documentación inválida o caducada.
- Pérdida de validez jurídica del solicitante (por ejemplo, renuncia o fallecimiento).
- Detección de riesgo, fraude o suplantación de identidad.
- Incumplimiento de términos y condiciones de uso. En caso de rechazo, se notificará formalmente al solicitante con una explicación general del motivo, respetando siempre la confidencialidad y normativa de protección de datos.

Las solicitudes rechazadas serán notificadas al Solicitante por correo electrónico, detallando la causa del rechazo. El Solicitante podrá enmendar y/o completar la Solicitud para que sea validada nuevamente.

5.2.3. Tiempo para procesar solicitudes de certificado

De conformidad con la Norma Técnica ARCOTEL-2024-0176, Art. 4, numeral 1, DICERT establece los siguientes límites de tiempo:

- El procesamiento de la solicitud, desde su recepción válida hasta la emisión o rechazo, se realizará en un plazo máximo de **15 días**.
- En casos donde se requieran validaciones adicionales, el solicitante será notificado y se podrá ampliar el plazo hasta por **10 días adicionales**.
- Las solicitudes automatizadas, sin incidencias, podrán ser procesadas en un plazo de **24 a 48 horas laborables** tras la recepción completa de la documentación, sujeto a la disponibilidad de los sistemas de verificación externos.

Todos los eventos del procesamiento quedan registrados en el sistema de trazabilidad de DICERT, asegurando cumplimiento normativo, auditoría posterior y evidencia para resolución de conflictos.

5.3. Emisión de Certificado[17]

Una vez completado exitosamente el proceso de validación y aprobación de la solicitud de certificado, la Autoridad de Certificación (AC) de DICERT ejecuta el proceso de emisión del certificado digital. Este proceso garantiza que la identidad del solicitante ha sido verificada de forma segura y conforme a las políticas de certificación vigentes.

5.3.1. Acciones de la AC durante la emisión

Una vez recibida la aprobación técnica de la AR, el sistema de la AC genera el certificado digital vinculando la clave pública del suscriptor con su identidad. El certificado es firmado por la Clave Privada de la AC Intermedia de DICERT.

5.3.2. Notificaciones al Suscriptor por parte de la CA sobre la Emisión del Certificado

Una vez emitido el certificado, DICERT envía un mensaje al correo electrónico registrado del titular, indicando que el certificado ha sido emitido exitosamente y proporcionando instrucciones para su descarga segura. La entrega del Certificado se realiza mediante los servicios y aplicaciones de DICERT.

5.4. Aceptación del Certificado[18]

[17] Atiende a la Sección 4.4.3 y 6 de la RFC 3647
[18] Atiende a la Sección 4.4.4 y 6 de la RFC 3647

5.4.1. Conducta que constituye la aceptación del certificado

La aceptación del certificado se considera efectiva cuando se firma el acta entrega-recepción (física o digitalmente) y no se ha presentado un reclamo por error o inexactitud al momento de su recepción, el certificado ha sido descargado del repositorio de DICERT, o utilizado por el suscriptor en cualquier transacción, comunicación o suscripción de un documento.

Al aceptar un Certificado, el Suscriptor se adhiere a las responsabilidades, obligaciones y deberes impuestos por el Contrato de Servicios y esta DPC, además declara y garantiza que:

- Sabe que ninguna persona no autorizada tiene acceso a la Llave Privada asociada al Certificado.
- La información provista durante el proceso de registro es auténtica y se refleja de manera correspondiente en el Certificado.
- Mantendrá control y confidencialidad de la Llave Privada correspondiente a la Llave Pública listada en el Certificado.
- Informará inmediatamente a DICERT en caso de cualquier evento que invalide o afecte la integridad del Certificado, como por ejemplo sospechas de pérdida, divulgación o cualquier otra afectación a la Llave Privada asociada.

5.4.2. Publicación del Certificado por la AC

DICERT publica el certificado en su repositorio interno para fines de gestión, y el estado del mismo queda disponible para consulta a través de los servicios OCSP.

5.4.3. Notificación de la Emisión del Certificado por parte de la AC a otras entidades.

DICERT mantiene los registros de emisión a disposición de ARCOTEL para fines de auditoría y control regulatorio. Cuando corresponda, DICERT notificará a terceros sobre la emisión de un certificado, como por ejemplo, la Autoridad de Registro que lo solicitó o entidades de control.

5.5. Uso de Pares de Claves y Certificados[19]

El uso adecuado y seguro del par de claves criptográficas (clave pública y clave privada), así como de los certificados emitidos por DICERT, es fundamental para garantizar la integridad, autenticidad y confianza en las transacciones electrónicas. Este apartado establece las obligaciones y responsabilidades tanto del suscriptor como de las partes confiables.

5.5.1. Uso del Certificado y Clave Privada del Suscriptor

El suscriptor debe usar la clave privada y el certificado solo para los fines autorizados en conformidad con esta DPC de DICERT y lo descrito en la Política de Certificación de DICERT.

[19] Atiende a la Sección 4.4.5 y 6 de la RFC 3647

El suscriptor se obliga a:

a. Emplear el certificado de acuerdo con lo establecido en este documento.
b. Ser especialmente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en esta DPC.
c. Comunicar a DICERT sin retrasos injustificables:
   i. La pérdida, el robo o el compromiso potencial de su clave privada.
   ii. La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación o por cualquier otra causa.
   iii. Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
d. El suscriptor debe dejar de utilizar la clave privada tras el término de vigencia, suspensión o revocación del certificado.
e. En caso de que el suscriptor entregue el acceso a sus datos de creación de firma a un tercero, los documentos electrónicos y/o las autenticaciones realizadas por estos terceros serán de su exclusiva responsabilidad, ya que el suscriptor sigue siendo responsable del uso que se haga de dichos datos. Esto es sin perjuicio del derecho de DICERT de tomar acciones civiles, administrativas o penales contra los terceros que hayan hecho uso indebido de los datos de creación de firma.

5.5.2. Uso de la clave pública y del certificado por parte de los terceros confiantes

Los terceros que confíen en los Certificados emitidos por DICERT, deben hacer uso del Certificado de conformidad con lo establecido en el campo de usos permitidos (“*keyUsage*“) y/o en la presente DPC.

Además, DICERT informa al tercero que confía en certificados que éste debe asumir las siguientes responsabilidades:

a. Disponer de suficiente información para tomar una decisión informada sobre si confiar o no en el certificado.
b. Ser el único responsable de decidir confiar o no en la información contenida en el certificado.
c. Asumir toda la responsabilidad en caso de incumplir con sus obligaciones como parte que confía en el certificado.

Las partes que confían **deben verificar la validez del certificado**, mediante los mecanismos habilitados por DICERT, como Protocolo OCSP y Consulta de la Lista de Certificados Revocados (CRL), antes de confiar en la información firmada. Además, deberán asumir toda la responsabilidad en caso de incumplir con sus obligaciones como parte que confía en el certificado.

5.6. Renovación de Certificados[20]

La renovación de un certificado digital consiste en la emisión de un nuevo certificado que mantiene los mismos datos del suscriptor y el mismo par de claves criptográficas, permitiendo extender la vigencia del certificado original sin modificaciones estructurales.

5.6.1. Circunstancias para la renovación de un certificado

No permitida por políticas de seguridad de la entidad.

5.6.2. Quién puede solicitar la Renovación

No estipulado.

5.6.3. Procesamiento de Solicitudes de Renovación de Certificados

No estipulado.

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

No estipulado.

5.6.5. Conducta que constituye aceptación de un certificado de renovación

No estipulado.

5.6.6. Publicación del certificado renovado por la AC

No estipulado.

5.6.7 Notificación de la emisión del certificado por la AC a otras entidades

No estipulado.

5.7. Regeneración de Claves (Re-key)

5.7.1. Circunstancias para la Renovación de la Clave del Certificado

Ver 4.3 de esta DPC.

5.7.2. Quién puede Solicitar la Certificación de una Nueva Clave Pública

Ver 4.3.1 de esta DPC.

[20] Atiende a la Sección 4.4.6 y 6 de la RFC 3647

5.7.3. Procesamiento de Solicitudes de Renovación de Claves de Certificado

Ver 4.3 de esta DPC

5.7.4. Notificación de la Emisión de un Nuevo Certificado al Titular

DICERT informará oficialmente al Titular del certificado que su certificado digital ha sido emitido de acuerdo con lo indicado en el punto 4.3 de esta DPC.

5.7.5. Conducta que Constituye Aceptación de un Certificado con Nueva Clave

Un certificado se considera aceptado por el Titular de acuerdo con lo descrito en el punto 5.4.1 de esta DPC.

5.7.6. Publicación del Certificado Renovado en la AC

DICERT publica los certificados emitidos en un repositorio de acceso público, conforme lo especificado en el punto 5.4.2. de esta DPC.

5.7.7. Notificación de la emisión del certificado por la AC a otras entidades

DICERT mantiene los registros de emisión a disposición de ARCOTEL para fines de auditoría y control regulatorio. Cuando corresponda, DICERT notificará a terceros sobre la renovación de un certificado, como por ejemplo, la Autoridad de Registro que lo solicitó o entidades de control.

5.8. Modificación de Certificado[21]

5.8.1. Circunstancias para la Modificación del Certificado

DICERT no permite modificar certificados ya emitidos. Cualquier solicitud de modificación del certificado será tratada como la solicitud de emisión de un nuevo certificado.

5.8.2. Quién puede solicitar la Modificación del Certificado

No estipulado.

5.8.3. Procesamiento de Solicitudes de Modificación del Certificado

No estipulado.

5.8.4. Notificación de la Emisión de un Nuevo Certificado al Titular

No estipulado.

[21] Atiende a la Sección 4.4.8 y 6 de la RFC 3647

5.8.5. Conducta que constituye aceptación de un certificado modificado

No estipulado.

5.8.6. Publicación del certificado modificado por la CA

No estipulado.

5.8.7. Notificación de la emisión del certificado por la AC a otras entidades

No estipulado.

5.9. Revocación y Suspensión de Certificados[22]

La revocación y la suspensión de certificados digitales emitidos por DICERT son mecanismos fundamentales para preservar la integridad y seguridad de la Infraestructura de Clave Pública (PKI), asegurando que los certificados no válidos o potencialmente comprometidos sean identificados y deshabilitados oportunamente. DICERT garantiza la disponibilidad de información actualizada y verificable sobre el estado de sus certificados, conforme a la normativa ecuatoriana y los estándares internacionales.

5.9.1. Circunstancias para la Revocación

DICERT permite a los usuarios solicitar en línea la **revocación inmediata** de sus certificados cuando detecten riesgos de uso indebido.

La revocación de un certificado implica dejar sin efecto su validez antes de la fecha de su caducidad. Este proceso es irreversible, es decir, una vez que un certificado es revocado ya no puede ser renovado o reactivado bajo ninguna circunstancia.

Es permitido realizar la revocación de certificados en los siguientes casos:

a. **Causas que afectan la seguridad de la llave o del certificado:**
   a.1. Si la clave privada del titular o la infraestructura utilizada en la emisión del certificado sufriera un incidente de seguridad que comprometa la fiabilidad de los certificados emitidos.
   a.2. En caso de que DICERT incurra en alguna infracción a los procedimientos y estándares de gestión de certificados definidos en este documento.
   a.3. Acceso no autorizado o uso indebido por un tercero de la llave privada del titular.
   a.4. Falta de diligencia en la custodia de la llave privada por parte del titular.

[22] Atiende a la Sección 4.4.9 de la RFC 3647

b. Causas que afectan al titular:

b.1. Infracción del titular en cuanto a sus obligaciones, responsabilidades y garantías establecidas en el contrato de servicios, los términos y condiciones, esta DPC o la Política de Certificación de DICERT.

b.2. Cuando DICERT tenga razones fundadas para considerar que ha existido pérdida, robo, modificación, divulgación no autorizada, o cualquier otra razón que comprometa la llave privada asociada con el certificado.

b.3. Fallecimiento o incapacidad del titular.

b.4. Disolución o liquidación de la persona jurídica titular de la firma.

c. Otras causas:

c.1. Por causa judicialmente declarada

c.2. Culminación del servicio por parte de DICERT.

c.3. El titular solicita por escrito que la AC revoque el certificado.

c.4. Si un certificado hubiera sido emitido como resultado de fraude o negligencia.

c.5. Cuando el certificado compromete el estado de confianza de DICERT.

c.6. Cuando se renueva un certificado.

c.7. Otras causas que puedan determinar las leyes o reglamentos.

La expiración del plazo de validez del certificado de firma electrónica surtirá efectos ipso facto, sin necesidad de iniciar un proceso de revocación.

La extinción de la firma electrónica no exime a su titular de las obligaciones previamente derivadas de su uso.

5.9.2. Quién puede solicitar la Revocación

La revocación de un certificado puede ser solicitada por la persona o titular a nombre del cual el certificado fue emitido; la Autoridad de Registro a nombre del titular del certificado; la Autoridad de Certificación y/o Registro a su nombre, solamente si tiene evidencia que justifique la revocación del certificado, si detecta algunos de las causas mencionadas en el punto 5.9.1 de esta DPC o de acuerdo con la solicitud de los tribunales de justicia; u otras personas determinadas por las leyes o reglamentos.

5.9.3. Procedimiento para la solicitud de Revocación

a. Solicitud de Revocación

A través del portal web público de **DICERT**, el titular del certificado puede iniciar la solicitud de revocación de su certificado digital. Para ello, debe seleccionar el certificado en cuestión, ingresar la causa de revocación y confirmar su identidad. Posteriormente, el sistema enviará un código de seguridad único al correo electrónico registrado por el titular. Si el titular ingresa el código de

seguridad correctamente, la solicitud de revocación se enviará automáticamente a la Autoridad de Certificación (AC) para su procesamiento.

b. Solicitud de revocación por la Autoridad de Registro

La Autoridad de Registro (AR) buscará el certificado correspondiente utilizando el número de documento de identidad o pasaporte del titular, o el identificador único de solicitud, señalando la causa de revocación. La solicitud de revocación se enviará directamente a la AC para su procesamiento, sin necesidad de pasos adicionales a la verificación de seguridad.

c. Procesamiento y actualización en la Lista de Certificados Revocados (CRL)

Una vez recibida y aprobada la solicitud de revocación por la AC, el certificado será añadido de inmediato a la Lista de Certificados Revocados (CRL). La CRL se actualiza conforme a los estándares de servicio para asegurar la disponibilidad pública y la verificación de los certificados revocados en tiempo real.

d. Notificación de Revocación

Al completarse el proceso de revocación, el sistema enviará automáticamente una notificación al correo electrónico del titular, confirmando la revocación exitosa del certificado. Esta notificación incluirá la fecha y hora de la revocación, así como información sobre el estado irreversible del proceso.

Asimismo, los terceros podrán conocer la revocación del certificado al consultar su validez mediante el número de serie del certificado.

e. Irreversibilidad de la Revocación

Ni el titular ni la Autoridad de Registro podrán solicitar la reactivación del certificado una vez que haya sido revocado, dado que la revocación es un proceso definitivo e irreversible. Cualquier necesidad futura de certificación requerirá la emisión de un nuevo certificado.

5.9.4. Plazo de gracia para la Solicitud de Revocación

Las solicitudes de revocación deben presentarse lo antes posible, dentro de un plazo razonable, el cual debe ser menor al plazo de vigencia del certificado; e, inmediatamente, tras conocer el compromiso de su clave. No existe período de gracia para el suscriptor en casos de compromiso de seguridad.

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

DICERT procesa la solicitud y actualizará su repositorio en un tiempo no mayor a **dos (2) horas** tras la recepción y validación de la solicitud.

5.9.6. Requisito de verificación de revocación para las partes confiantes

Los terceros que confían deben confirmar la validez de cada Certificado en la cadena de certificados chequeando la CRL o respuesta OCSP respectiva, antes de depositar su confianza en un Certificado emitido por DICERT.

5.9.7. Frecuencia de Emisión de CRL

Las Listas de Certificados Revocados (CRL) son emitidas y actualizadas por lo menos 1 vez cada 24 horas, garantizando la actualización continua de los datos sobre certificados revocados y suspendidos.

En casos excepcionales, como revocaciones críticas, DICERT emite CRLs de emergencia antes del vencimiento de la lista actual.

Cada CRL está identificada con un número secuencial único que asegura su autenticidad y rastreo.

5.9.8. Latencia máxima de la CRL

Las Listas de Revocación de Certificados (CRL) se publican en el repositorio en un tiempo razonable después de su generación, generalmente en unos quince (15) minutos como máximo.

5.9.9. Disponibilidad de Comprobación de estado/revocación en Línea

DICERT hace disponible información de estatus OCSP para todos sus certificados. La ubicación del servidor OCSP se incluye en el certificado respectivo.

Las respuestas OCSP se hacen conforme a los estándares RFC6960 y FFC5019. Estas cumplen con al menos una de las siguientes:

1. Está firmada por la AC que emitió los Certificados de los cuales se indica el estatus de revocación, o
2. Está firmada por un Servidor OCSP cuyo Certificado fue firmado por la AC que emitió los Certificados cuyo estatus de revocación se indica.

5.9.10. Requisitos de Comprobación de Revocación en Línea

Una Parte que confía debe verificar el estado del certificado en el cual desea confiar. Si dicha Parte que Confía no verifica el estado del certificado mediante la consulta de la Lista de Revocación de Certificados (CRL) más reciente, deberá hacerlo consultando el Estado del Certificado utilizando el servicio OCSP.

El Servidor OCSP soporta la recepción de solicitudes OCSP mediante el método GET. No responde una respuesta de estatus “válido” a certificados que no hayan sido emitidos. Para Certificados en general, se actualiza inmediatamente luego de la emisión del mismo. Tiene una validez mínima de un día y una validez máxima de siete días.

5.9.11. Otras formas de Anuncios de Revocación Disponibles

No aplica.

5.9.12. Requisitos especiales en caso de compromiso de clave privada

En el evento crítico de que la clave privada de la **AC de DICERT** (o de su AC Raíz) sea comprometida, se sospeche de su uso no autorizado, o los algoritmos criptográficos pierdan su integridad (por ejemplo, por un avance en criptoanálisis), se seguirán estos requisitos especiales:

a. **Notificación Inmediata:** Se informará a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) en un plazo no mayor a 24 horas.
b. **Revocación Masiva:** Se procederá a la revocación de todos los certificados vigentes que dependan de dicha clave comprometida.
c. **Comunicación Pública:** Se publicará un aviso destacado en el sitio web de DICERT y se enviará una notificación masiva a todos los suscriptores y partes confiantes.

d. **Cese de Emisión:** La AC cesará inmediatamente la emisión de nuevos certificados hasta que se genere un nuevo par de claves bajo una ceremonia de claves auditada.

5.9.13 Circunstancias para la Suspensión

El efecto de la suspensión del certificado es el cese temporal de los efectos jurídicos del mismo conforme a los usos que le son propios e impide el uso legítimo del mismo por parte del Titular y es reversible.

La suspensión aplica a aquellos certificados que están en estado Vigente, y que por lo tanto no se encuentran revocados y no se ha cumplido su periodo de vigencia.

La reactivación de un certificado supone su paso de estado suspendido a estado vigente, siempre y cuando no se haya cumplido su periodo de vigencia.

5.9.14. Quién puede solicitar la Suspensión

La normativa ecuatoriana contempla la suspensión, pero DICERT **no ofrece el servicio de suspensión temporal** para evitar ambigüedades en la responsabilidad legal. Todo proceso de cese de validez es definitivo (revocación).

5.9.15. Procedimiento para solicitud de Suspensión

No estipulado.

5.9.16. Límite de Tiempo para la Suspensión

No estipulado.

5.10. Servicios de Estatus de Certificados[23]

5.10.1 Características Operativas

DICERT proporciona información sobre el estado de los certificados (válido, revocado o expirado) a través de dos mecanismos principales:

1. **Listas de Revocación de Certificados (CRL):** Archivos firmados por la AC que contienen los números de serie de los certificados revocados.
2. **Protocolo de Estado de Certificados en Línea (OCSP):** Un servicio de consulta interactiva que devuelve el estado actual del certificado de forma inmediata.

Los registros de revocación en una CRL o Respuesta OCSP no se eliminan hasta después de la Fecha de Expiración del Certificado que fue revocado, para la consulta de la parte que confía.

No obstante, los registros quedan almacenados en los repositorios de DICERT, durante el tiempo de la acreditación de DICERT.

5.10.2. Disponibilidad del Servicio

Los servicios de consulta de estado (OCSP y repositorio de CRL) están disponibles de forma permanente **(24 horas al día, 7 días a la semana)**. DICERT cuenta con infraestructura redundante para garantizar que los terceros confiantes puedan verificar la validez de las firmas en cualquier momento.

5.10.3. Características Opcionales

El servicio OCSP es una opción sistémica para verificar el estado de los certificados, que complementa la funcionalidad de la CRL.

5.11. Fin de la Suscripción[24]

La suscripción termina cuando el certificado expira o cuando el certificado haya sido revocado. Una suscripción también se da por terminada cuando el contrato respectivo expire o no se renueve.

5.12. Custodia y Recuperación de Claves[25]

[23] Atiende a la Sección 4.4.10 y 6 de la RFC 3647
[24] Atiende a la Sección 4.4.11 y 6 de la RFC 3647
[25] Atiende a la Sección 4.4.12 y 6 de la RFC 3647

DICERT no custodia ni almacena las claves privadas de firma electrónica de los suscriptores. Por lo tanto, no existe un procedimiento de recuperación de claves. En caso de pérdida de la clave privada o del dispositivo (Token/HSM), el suscriptor debe solicitar la revocación y una nueva emisión.

5.12.1 Política y prácticas de Depósito y Recuperación de Llaves

No estipulado.

5.12.2 Política y Prácticas de Encapsulamiento y Recuperación de Llaves de Sesión

No estipulado.

6. Controles Gestión, Operativos y Físicos[26]

6.1. Controles de Seguridad Física

La infraestructura de DICERT es operada por instalaciones seguras de DICERT DISTRIBUIDORA INTERNACIONAL DE CERTIFICACIÓN ELECTRÓNICA S.A., operadas por Amazon Web Services Inc. El acceso no autorizado a las instalaciones donde opera DICERT está prohibido por los procedimientos de seguridad respectivos.

6.1.1. Localización del Sitio y Construcción

DICERT utiliza la infraestructura de Amazon Web Services (AWS) en regiones y zonas de disponibilidad diseñadas específicamente para alta seguridad y resiliencia. La construcción de estos centros de datos cumple con normativas internacionales de resistencia estructural y protección contra desastres.

6.1.2. Acceso Físico

DICERT implementa controles de seguridad física apropiados para restringir el acceso a todo el hardware y software utilizado para proporcionar los servicios de AC. El acceso a dicho hardware y software está limitado al personal que desempeña un rol de confianza como se describe en la *Sección 6.2.1* de esta DPC.

El acceso se controla mediante el uso de controles de acceso electrónicos, juegos de cerraduras de combinación mecánica, cerrojos u otros mecanismos de seguridad. Dichos controles de acceso se controlan manual o electrónicamente para detectar intrusiones no autorizadas en todo momento.

Solo el personal autorizado podrá acceder, ya sea físico o lógico, a los sistemas desde los cuales opera la AC. El acceso físico está limitado a personal autorizado de Amazon Web Services Inc.,

[26] Atiende a la Sección 4.5. y 6 de la RFC 3647

exclusivamente para tareas de mantenimiento, cumpliendo con los más altos estándares de seguridad.

Los servidores de DICERT se encuentran dentro de un gabinete cerrado o área de jaula en una sala de servidores cerrada. El acceso a la sala del servidor está controlado por lectores de credenciales. Las claves privadas para las AC se almacenan en módulos de seguridad de hardware que están validados para FIPS 140-2 Nivel 3 o superior y que son físicamente evidentes y resistentes a la manipulación, de acuerdo con las políticas que maneja Amazon Web Services Inc.

6.1.3. Energía y Aire Acondicionado

DICERT hereda los sistemas de redundancia de AWS (N+1), que incluyen múltiples fuentes de energía, generadores de respaldo y sistemas de refrigeración de precisión que garantizan la operatividad continua de la AC.

6.1.4. Exposición al Agua

AWS selecciona ubicaciones de centros de datos con bajo riesgo de inundación y emplea sistemas de detección y prevención de humedad en todas sus salas.

6.1.5. Prevención y Protección contra Incendios

La infraestructura cuenta con sistemas de supresión de incendios automatizados de última generación, supervisados las 24 horas.

6.1.6. Almacenamiento de Medios

DICERT utiliza servicios de almacenamiento en la nube (como Amazon S3) con cifrado en reposo y políticas de versionamiento, además de copias de seguridad en diferentes regiones geográficas.

6.1.7. Eliminación de Residuos

AWS sigue procedimientos estrictos de desmagnetización y destrucción física de medios de almacenamiento que han llegado al final de su vida útil, conforme al estándar NIST SP 800-88.

6.1.8. Copias de Seguridad fuera del Sitio

Se garantiza la disponibilidad mediante la replicación de datos en múltiples zonas de disponibilidad (Multi-AZ) y regiones distintas, asegurando la recuperación ante desastres de gran escala.

6.2. Controles de Procedimientos[27]

DICERT asegura que los sistemas de la infraestructura tecnológica operen de manera segura mediante procedimientos específicos para las funciones que afectan la provisión de servicios de certificación.

El personal responsable de la prestación del servicio sigue los procedimientos administrativos y de gestión conforme a la Política de Seguridad de la Información de DICERT.

6.2.1. Roles de Confianza

El personal que tiene acceso o control sobre las operaciones criptográficas en DICERT que afecten la emisión, uso y gestión de Certificados se consideran sirviendo bajo un "Rol de Confianza". Este personal incluye, pero no está limitado a, miembros del equipo de Autoridad de Certificación de DICERT.

6.2.2. Número de personas requeridas para una tarea

Se aplica estrictamente el principio de Control Mutuo (regla de dos personas o esquema *m de n*) para las siguientes actividades críticas:

- Generación, activación y respaldo de las claves privadas de la AC en el CloudHSM.
- Restauración de sistemas tras un desastre.
- Cambios significativos en la configuración de seguridad de la red VPC.

Este mismo criterio se aplica a la ejecución de tareas como la emisión y activación de certificados, así como a cualquier manipulación del dispositivo que custodia las claves de la Autoridad de Certificación raíz e intermedias.

6.2.3. Identificación y Autenticación de cada Rol

DICERT mantiene controles que aseguran de manera razonable que:

a. Se sigue un procedimiento documentado para embestir personas en un Rol de Confianza y asignar las responsabilidades correspondientes;
b. Sólo personal que tenga asignado un Rol de Confianza tendrá acceso a Zonas Seguras y Zonas de Alta Seguridad;
c. Personas en un Rol de Confianza actúan bajo ese rol únicamente cuando realicen actividades administrativas;
d. Empleados y contratistas externos observan el principio del Mínimo Privilegio cuando accedan o configuren accesos a los Sistemas de Certificados;
e. Cuando un Rol de Confianza utilice un usuario y contraseña para autenticarse, los controles de acceso están configurados de tal manera que se satisfagan los siguientes requerimientos:

[27] Atiende a la Sección 4.5.2 de la RFC 3647

- Las contraseñas tienen al menos doce (12) caracteres para cuentas internas (accesibles solo desde Zonas Seguras o Zonas de Alta Seguridad);
- Las contraseñas de cuentas accesibles desde fuera de Zonas Seguras o Zonas de Alta Seguridad son configuradas para tener al menos ocho (8) caracteres y una combinación de al menos un número y caracteres alfabéticos, evitando que sea una de las cuatro últimas contraseñas utilizadas; e implementar bloqueo de la cuenta por intentos de acceso fallidos;

f. Los Roles de Confianza cierran sesión en su computador cuando no la están usando;
g. Las Estaciones de Trabajo están configuradas con detectores de inactividad que cierran la sesión del usuario automáticamente;
h. Se revisan todos los sistemas al menos cada 90 días y se desactivan cuentas que ya no sea necesario mantener en operación;
i. Revocar el acceso a Sistemas de Certificados a cuentas que superen los cinco (5) intentos de acceso no autorizados;
j. Desactivar todos los privilegios de acceso individuales a los Sistemas de Certificados en un plazo máximo de 24 horas luego del fin de la relación laboral de determinado empleado con la AC.
k. Aplicar múltiples factores de autenticación para accesos de administrador a los Sistemas de Emisión y Sistemas de Administración de Certificados;
l. Restringir el acceso remoto o el acceso a los Sistemas de Emisión, Sistemas de Administración de Certificados o Sistemas de Seguridad excepto cuando:
    - La conexión remota se origine de un dispositivo de propiedad y/o controlado por la AC desde una IP externa pre-aprobada;
    - El acceso remoto se realice mediante un canal seguro y cifrado, de carácter temporal y no persistente que soporta autenticación de dos factores;
    - La conexión remota es realizada a un dispositivo intermedio que cumple con lo siguiente:
        ■ Está localizado en la red de la AC.
        ■ Está asegurado conforme a los requerimientos de esta DPC, y
        ■ Actúa como intermediario para la conexión remota con el Sistema de Emisión.

6.2.4. Roles que requieren separación de funciones

Los roles que requieren separación de funciones incluyen:

a. 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 confianza.
b. Emisión, suspensión y revocación de certificados, serán tareas incompatibles con la Administración y operación de los sistemas.

c. La administración de los sistemas, así como la activación de una CA en un ambiente de producción es incompatible con las funciones del Operador de registro y Auditor.

Para verificar la conformidad con las políticas y procedimientos aplicables, DICERT realiza auditorías independientes anuales.

6.3. Controles de Seguridad del Personal[28]

6.3.1. Requisitos de calificaciones, experiencia y autorizaciones

Todo el personal de DICERT está adecuadamente calificado y/o instruido para desempeñar las operaciones asignadas. DICERT ha implementado políticas para verificar la identidad e integridad de su personal. DICERT asegura que los Operadores de Registro sean confiables para llevar a cabo las tareas de registro, proporcionándoles formación para ejecutar correctamente los procesos de Comprobación fehaciente de identidad de los solicitantes. Adicionalmente, DICERT evalúa el desempeño del equipo de la AC para asegurarse que desempeñan sus tareas de manera satisfactoria.

Con todo, las Autoridades de Registro pueden establecer procedimientos adicionales de verificación de antecedentes, siempre que se alineen con la legislación vigente, las políticas de DICERT, y son responsables por las acciones de las personas a las que autoricen en sus operaciones.

6.3.2. Procedimientos de verificación de antecedentes

DICERT sigue un grupo de procedimientos para seleccionar y evaluar personal que opera la AC o actúa en cualquier otro rol relacionado a seguridad de la información.

DICERT antes de contratar a una persona o permitir que acceda al puesto de trabajo, se llevan a cabo las siguientes verificaciones:

a. Referencias de empleos anteriores.
b. Nivel de estudios.

Todas las verificaciones se realizan dentro de los límites establecidos por la legislación vigente aplicable.

6.3.3. Requisitos de capacitación

Todo el personal de DICERT que realiza tareas de verificación de información recibe capacitación en habilidades que cubre el conocimiento básico de Infraestructura de Clave Pública, políticas y procedimientos de autenticación y verificación (incluida esta DPC), amenazas comunes al proceso de verificación de información, incluido el phishing y otras tácticas de ingeniería social, las Políticas y procedimientos de seguridad de la información de DICERT, incluyendo el uso y operación de equipos y aplicaciones instaladas, la gestión y manejo de incidentes y compromisos de seguridad de la

[28] Atiende a la Sección 4.5.3. de la RFC 3647

información, los procedimientos de continuidad de negocio y de emergencia, y los procedimientos de gestión y seguridad relacionados con el tratamiento de datos personales.

Los especialistas en validación reciben su capacitación de habilidades antes de comenzar su trabajo y DICERT les exige que aprueben un examen sobre los requisitos de verificación de información aplicables.

Los programas de formación se revisan periódicamente y se actualizan para mejorarlos de manera continua.

DICERT mantiene registros de capacitación y se asegura de que el personal encargado de las tareas de un especialista en validación, mantenga un nivel de habilidad adecuado.

6.3.4. Frecuencia y requisitos de actualización de la formación

DICERT realiza una actualización técnica semestral y formación en concienciación de seguridad anual.

6.3.5. Frecuencia y secuencia de Rotación de Personal

Se aplican auditorías cruzadas en lugar de rotación frecuente para mantener la especialización técnica sin comprometer la seguridad.

6.3.6. Sanciones por acciones no autorizadas

DICERT impone sanciones, incluyendo la suspensión y/o despido si es apropiado, a sus empleados en roles de confianza si ellos realizan actos no autorizados, abusan de su autoridad; o por cualquier otra razón apropiada, de conformidad con el Reglamento Interno y Código de Ética de la AC.

6.3.7. Requisitos para contratistas independientes

Los contratistas independientes deben cumplir con los mismos requerimientos que los empleados de DICERT.

DICERT puede contratar a terceros para desempeñar tareas de confianza, quienes previamente deben firmar las cláusulas de confidencialidad, de responsabilidad civil y cumplir con los requisitos operativos establecidos por DICERT. Cualquier acción que comprometa la seguridad de los procesos aceptados podría, resultar en la terminación del contrato y habilita a DICERT para ejercer las acciones legales correspondientes.

En el caso de que todas o parte de las operaciones de certificación sean realizadas por un tercero, dicho tercero debe aplicar y cumplir con los controles y disposiciones establecidos en esta sección u otras partes de la DPC. Sin embargo, DICERT sigue siendo responsable de asegurar la ejecución efectiva de estas medidas. Estos aspectos están formalizados en el acuerdo legal utilizado para la prestación de servicios por un tercero con DICERT.

6.3.8. Documentación suministrada al personal

DICERT provee a sus empleados el entrenamiento y documentación necesarios para ejecutar su rol de trabajo de manera competente y satisfactoria. En particular, se da acceso a los manuales de funciones, esta DPC y las Políticas de Seguridad de la Información.

6.4. Procedimientos de Registro de Auditorías[29]

6.4.1. Tipos de Eventos Registrados

DICERT registra todos los eventos del sistema y las aplicaciones de la AC y crea registros de gestión de certificados a partir de los datos recopilados de acuerdo con los procedimientos de auditoría interna. Se registran los siguientes eventos:

a. Eventos clave de gestión del ciclo de vida de la AC:
   - Generación de claves, copia de seguridad, almacenamiento, recuperación, archivo y destrucción;

b. Eventos de solicitante y suscriptor:
   - Solicitud para crear un certificado;
   - Solicitud de revocación de un certificado.

c. Eventos del ciclo de vida del certificado de AC y del suscriptor
   - Actividades de verificación estipuladas en esta DPC;
   - Aceptación y rechazo de solicitudes de certificados, frecuencia de registro de procesamiento;
   - Generación de claves;
   - Notificación de compromiso clave;
   - Creación de un certificado;
   - Entrega de un certificado;
   - Revocación de un certificado;
   - Generación de una lista de revocación de certificados;
   - Generación de una respuesta OCSP;

d. Acciones del personal de confianza
   - Eventos de inicio de sesión y uso de mecanismos de identificación y autenticación;
   - Cambios a las políticas de AC;
   - Cambios a las claves de AC;
   - Cambios de configuración a la AC.

e. Eventos de seguridad
   - Intentos exitosos y fallidos de acceso al sistema PKI;
   - PKI y acciones del sistema de seguridad realizadas;
   - Cambios de perfil de seguridad;
   - Fallos del sistema, fallas de hardware y otras anomalías;

[29] Atiende a la Sección 4.5.4. y 6 de la RFC 3647

- Actividades de firewall y enrutador;
- Entradas y salidas de la instalación de AC.

f. Las entradas de registro incluyen los siguientes elementos:
- Fecha y hora de entrada;
- Identidad de la persona que hace la entrada del diario; y
- Descripción de la entrada.

DICERT recopila información de eventos y crea registros de gestión de certificados mediante procedimientos automatizados. Cuando esto no sea posible, se pueden utilizar los métodos manuales de registro y mantenimiento de eventos.

6.4.2. Frecuencia de Procesamiento de Registros

Los sistemas de monitoreo generan alertas en tiempo real (Amazon CloudWatch). El Oficial de Seguridad revisa los reportes de anomalías de forma semanal.

El procesamiento de los registros de auditoría implica una revisión para asegurar que no hayan sido manipulados, una inspección rápida de todas las entradas de registro, y una investigación detallada de cualquier alerta o irregularidad encontrada. Todas las acciones tomadas como resultado de la revisión de auditoría se deben documentar en cumplimiento con la ***política de gestión de incidentes*** de DICERT.

6.4.3. Período de Retención de Registros de Auditoría

DICERT retiene cualquier registro de auditoría durante un periodo de hasta 10 años, o más si es requerido por la ley, dependiendo del tipo de información registrada. Estos registros están disponibles a través de métodos automatizados.

6.4.4. Protección de los Registros de Auditoría

Los registros de auditoría estarán protegidos mediante medios electrónicos para garantizar la integridad, la identificación temporal y el seguimiento de las actividades. Esto incluye la implementación de mecanismos para proteger los archivos de registro contra modificaciones, eliminaciones no autorizadas u otros tipos de manipulación.

6.4.5. Procedimientos de Respaldo de Registros de Auditoría

Dispone de un procedimiento de respaldo adecuado para asegurar que, en caso de pérdida o destrucción de archivos relevantes, las copias de respaldo correspondientes de los registros estén disponibles en un período corto de tiempo.

6.4.6. Sistema de Recolección de Registros de Auditoría (interno vs. externo)

Los registros de auditoría son recolectados y tratados en los sistemas internos de la AC, de manera automática y manual, de conformidad con esta DPC y la ***política de gestión de incidentes*** de DICERT.

6.4.7. Notificación al sujeto causante del evento

Cuando el sistema de registro de auditoría registre un evento, no es necesario enviar una notificación al individuo, organización, dispositivo o aplicación responsable del evento.

Los eventos que sean considerados potenciales problemas de seguridad relacionados a la infraestructura de la AC serán escalados a un equipo de monitoreo permanente de seguridad.

6.4.8. Evaluaciones de Vulnerabilidad

DICERT cuenta con una ***política de gestión de vulnerabilidades técnicas*** en base a la que se realizan evaluaciones, de caracter preventivo y reactivo. Los sistemas de recolección de registros, están programados para generar alertas automáticas en los casos configurados según la política mencionada.

El equipo de seguridad, interviene para realizar evaluaciones de vulnerabilidad, cuando de conformidad con la política de gestión de vulnerabilidades, se requiera. En todo caso, anualmente el equipo de seguridad de DICERT realiza una revisión del cumplimiento del sistema de gestión de seguridad de la información, así como la gestión de auditorías externas para llevar a cabo test de penetración, análisis estático y dinámico de desarrollos e infraestructura tecnológica.

6.5. Archivo de Registros[30]

6.5.1. Tipos de Registros Archivados

Los registros que se archivan son los especificados en la ***Sección 6.4.***

6.5.2. Periodo de Retención para Archivo

DICERT almacena la información de los registros durante un periodo de hasta 10 años, o más si es requerido por la ley, dependiendo del tipo de información registrada, en concordancia con lo establecido en el ***punto 6.4.3*** de esta DPC.

6.5.3 Protección del Archivo

El archivo se protege mediante:

- **Cifrado en reposo:** Uso de AWS KMS (Key Management Service) con algoritmos AES-256.
- **Inmutabilidad:** Uso de políticas de *Object Lock* en Amazon S3 para evitar la eliminación o modificación accidental o maliciosa.

[30] Atiende a la Sección 4.5.5. y 6 de la RFC 3647

- **Control de acceso:** Restricción estricta mediante políticas IAM (Identity and Access Management).

6.5.4. Procedimientos de Respaldo del Archivo

Los procedimientos de copia de seguridad y recuperación existen y pueden utilizarse para que esté disponible un conjunto completo de copias de seguridad en caso de pérdida o destrucción de los archivos primarios.

6.5.5. Requisitos para Sellado de Tiempo de Registros

Todos los eventos registrados cuentan con una estampa de tiempo sincronizada mediante el protocolo NTP con fuentes de tiempo de alta precisión de AWS, asegurando la trazabilidad cronológica de las operaciones.

6.5.6. Sistema de Recopilación de Archivos (interno o externo)

DICERT utiliza un sistema de recopilación **interno** gestionado sobre infraestructura de AWS, centralizando los logs en un repositorio seguro y auditado.

6.5.7. Procedimientos para obtener y verificar información de archivo

Sólo personal de confianza autorizado de DICERT puede obtener acceso al archivo. La integridad de la información es verificada cuando el archivo se recupera desde los registros archivados.

6.6. Cambio de Claves[31]

El procedimiento para proporcionar un nuevo certificado de AC a un Sujeto después de la generación de una nueva clave es el mismo que el procedimiento para proporcionar inicialmente el certificado de la AC.

6.7. Compromiso y Recuperación ante Desastres[32]

6.7.1. Procedimientos de manejo de incidentes y compromisos

DICERT ha desarrollado la ***Política de Seguridad de la Información*** y la ***Política de Continuidad del Negocio*** que son desarrollados por *Planes de Respuesta a Incidentes* y de *Recuperación ante Desastres*, mismos que establecen los procedimientos para gestionar y recuperar los sistemas en caso de incidentes y compromisos de sus operaciones, asegurando la disponibilidad de los servicios críticos de emisión, revocación y publicación del estado de los certificados.

[31] Atiende a la Sección 4.5.6. y 6 de la RFC 3647
[32] Atiende a la Sección 4.5.7. y 6 de la RFC 3647

6.7.2. Recursos informáticos, software y/o datos corruptos

En caso de corrupción de datos o falla de software en AWS, DICERT activará el Plan de Recuperación de Desastres (DRP), restaurando los servicios desde imágenes de servidor (AMIs) y bases de datos respaldadas en regiones seguras.

6.7.3. Procedimientos de recuperación ante el compromiso clave privada de la entidad

En el evento de que la clave privada de una Autoridad de Certificación (AC) de DICERT se vea comprometida, la entidad actúa de forma inmediata para:

a) Suspender de forma inmediata el uso del material criptográfico afectado;
b) Revocar todos los certificados que hayan sido firmados con dicha clave;
c) Implementar acciones razonables desde el punto de vista comercial para informar a todos los suscriptores sobre la revocación;
d) Y asegurar que los suscriptores cesen el uso de los certificados afectados para cualquier fin.

Una vez que se haya reemplazado el material criptográfico comprometido y restablecido la operación segura de la AC correspondiente, DICERT podrá proceder a emitir nuevamente los certificados revocados, conforme al mismo procedimiento utilizado en la emisión original.

6.7.4. Capacidades de continuidad comercial después de un desastre

Como parte de su estrategia de respuesta, DICERT emplea y contrata personal especializado en seguridad, capacitado para ejecutar acciones inmediatas de monitoreo y control sobre las instalaciones, la infraestructura tecnológica y los servicios esenciales de la AC tras la ocurrencia de un desastre. El objetivo principal es mitigar cualquier pérdida, evitar daños adicionales y prevenir el acceso no autorizado o robo de materiales sensibles e información crítica.

Adicionalmente, para validar su capacidad de recuperación, DICERT realiza pruebas al menos una vez al año de sus planes de continuidad del negocio y recuperación ante desastres. Estas pruebas permiten identificar oportunidades de mejora, garantizar la efectividad de los procedimientos establecidos y asegurar que el personal involucrado esté adecuadamente preparado para actuar ante situaciones reales de emergencia.

Este enfoque proactivo permite a DICERT minimizar el tiempo de inactividad, mantener la confianza de sus clientes y partes interesadas, y garantizar la continuidad de los servicios de certificación digital incluso en condiciones adversas.

6.8. Terminación de una AC o AR[33]

Cuando sea necesario terminar la operación de una AC de DICERT, el impacto de la terminación se debe minimizar lo más posible dadas las circunstancias. Esto incluye:

a. Notificar a ARCOTEL con al menos 90 días de anticipación.
b. Proporcionar aviso previo factible y razonable a todos los Suscriptores;
c. Ayudar con la transferencia ordenada del servicio y los registros operativos a una AC sucesora, de existir alguna;
d. Preservar todos los registros por mínimo un (1) año o según lo requiera esta DPC, o lo que sea más largo. La identidad del custodio de estos registros se describen en la sección 1 de esta DPC; y
e. Revocar todos los certificados emitidos por la AC, a más tardar en el momento de la terminación.
f. Se destruirán las claves privadas de la AC de forma segura y auditada.

7. Controles Técnicos de Seguridad[34]

7.1. Generación de par de Llaves e Instalación

7.1.1. Generación de par de Llaves

Los pares de claves para las AC de DICERT se generan de conformidad con los procedimientos formales de generación de claves y dentro de un Módulo de Seguridad de Hardware certificado FIPS 140-2 Nivel 3 del que no se puede extraer la clave privada en texto sin formato.

Las solicitudes de certificados de suscriptor se rechazan si la clave pública no cumple con los requisitos establecidos en las *Secciones 7.1.5* y *7.1.6* o si tiene una clave privada débil conocida.

7.1.2. Entrega de Clave Privada al Suscriptor

Los Certificados son emitidos en formato PKCS#12 y la clave privada se encuentra contenida en un archivo que el suscriptor podrá acceder a través de su cuenta en el portal de gestión de certificados de DICERT. La contraseña del archivo es escogida por el suscriptor, cumpliendo con las prácticas de seguridad de esta DPC.

7.1.3. Entrega de Clave Pública al Emisor del Certificado

Los suscriptores proporcionan su llave pública a DICERT para la certificación a través de una Solicitud de firma de certificado (CSR). El método de transferencia único para enviar esta información es

[33] Atiende a la Sección 4.5.8. y 6 de la RFC 3647
[34] Atiende a la Sección 4.6. y 6 de la RFC 3647

HTTPs sobre Secure Sockets Layer (SSL). Es obligación del suscriptor proteger la clave que configura al tiempo de realizar el CSR.

7.1.4. Entrega de clave pública de AC a Terceros que Confían

Las claves públicas de las AC de DICERT están disponibles en el repositorio en línea en https://dicert.com.ec/links/certac. El método de transferencia único para enviar esta información es HTTPs sobre Secure Sockets Layer (SSL).

7.1.5. Tamaños de Claves

Para evitar ataques criptoanalíticos, todas las AC de DICERT utilizan tamaños de clave y protocolos criptográficos que se adhieren a las recomendaciones del NIST y a las disposiciones aplicables de los Requisitos de Referencia, como Sha256 con encriptación RSA 2048.

7.1.6. Generación de Parámetros de Clave Pública y Control de Calidad

Para las claves RSA, DICERT confirma que el valor del exponente público es un número impar igual a 3 o más. Se verifican otros parámetros criptográficos como la entropía, la primalidad de los factores, y la validez de los parámetros en caso de usar algoritmos como DSA.

7.1.7. Propósitos de Uso de Claves (según X.509 v3. Campo de uso de claves)

Las claves incluidas en los certificados emitidos por DICERT están restringidas a los usos definidos en las extensiones keyUsage y extendedKeyUsage de los certificados X.509 v3.

Estos propósitos incluyen, pero no se limitan a: firma digital, autenticación de cliente, autenticación de servidor, cifrado de clave, y protección de correo electrónico seguro. Las restricciones de uso se establecen en función del tipo de certificado emitido.

7.2. Protección de Clave Privada y Controles de Ingeniería del Módulo Criptográfico[35]

7.2.1. Estándares y controles del Módulo Criptográfico

Todas las claves privadas de la AC utilizadas para firmar certificados, CRL o cualquier información relacionada utilizan módulos de seguridad de hardware que cumplen con el estándar FIPS 140-2 Nivel 3 o superior y las especificaciones de seguridad Common Criteria EAL4 +. La criptografía aplicada para proteger esta información está seleccionada para resistir ataques criptoanalíticos durante la vida útil de la clave cifrada.

[35] Atiende a la Sección 4.6.2 y 6 de la RFC 3647

Las claves privadas de la AC se guardan en una ubicación físicamente segura y nunca se almacenan sin cifrar fuera de los módulos de seguridad de hardware.

7.2.2. Control multipersona de la Llave Privada (n de m)

La activación de claves de la AC requiere un quórum de al menos 2 de n personas en roles de confianza.

7.2.3. Custodia de Clave Privada

La AC no custodia claves de firma de suscriptores. Las de la AC residen en el HSM.

7.2.4. Copia de Seguridad de Clave Privada

DICERT realiza copias de respaldo de las claves privadas de las CAs para asegurar su recuperación en caso de desastre, pérdida o deterioro. El procedimiento de respaldo de las claves privadas de la AC se encuentra declarado en el *Plan de Administración de Llaves Criptográficas*, el que es de uso confidencial de DICERT.

7.2.5. Archivo de Clave Privada

Las claves privadas que pertenecen a las AC de DICERT no son archivadas por terceros que no sean DICERT.

DICERT no mantiene copias de las llaves privadas del Titular.

7.2.6. Transferencia de Clave Privada hacia o desde un Módulo Criptográfico

Todas las transferencias de claves privadas hacia o desde un módulo criptográfico se realizan de acuerdo con los procedimientos especificados por el proveedor del módulo criptográfico.

7.2.7. Almacenamiento de Clave Privada en Módulo Criptográfico

Las claves privadas se almacenan de acuerdo con las instrucciones aplicables especificadas por el fabricante del módulo criptográfico.

7.2.8. Método de Activación de Clave Privada

Las claves privadas se activan de acuerdo con las instrucciones aplicables especificadas por el fabricante del módulo criptográfico.

7.2.9. Método de Desactivación de Clave Privada

Las claves privadas se desactivan de acuerdo con las instrucciones aplicables especificadas por el fabricante del módulo criptográfico.

7.2.10. Método de Destrucción de Clave Privada

Las claves privadas se destruyen de acuerdo con las instrucciones aplicables especificadas por el fabricante del módulo criptográfico. Además, se sigue el *Plan de Administración de Llaves Criptográficas* de DICERT, el que es de uso confidencial.

7.2.11. Clasificación del Módulo Criptográfico

Ver *Sección 7.2.1.*

7.3. Otros Aspectos de la Gestión de pares de Claves[36]

7.3.1. Archivo de la Clave Pública

DICERT archiva las claves públicas y certificados por 10 años.

7.3.2. Periodos operativos de certificado y períodos de uso de pares de claves

Los certificados son válidos desde el momento de la firma, a menos que se especifique lo contrario en la estructura de validez del certificado, hasta el final indicado en el tiempo de vencimiento del certificado.

Los Certificados de Suscriptores se emiten por un período de 24 horas, 8 días, 15 días, uno, dos, tres o cinco años.

7.4. Datos de Activación[37]

7.4.1. Generación e Instalación de Datos de Activación

Passphrases creadas por el suscriptor siguiendo políticas de complejidad (8+ caracteres, alfanuméricos).

7.4.2. Protección de Datos de Activación

Las claves del Módulo de seguridad de hardware se almacenan en el Módulo de seguridad de hardware y solo pueden ser utilizadas por administradores autorizados de la AC tras la autenticación respectiva. Las contraseñas necesarias para desbloquear las claves se almacenan en forma cifrada.

De cara al titular, la responsabilidad es exclusiva de este. DICERT no conoce ni almacena estos datos.

[36] Atiende a la Sección 4.6.3 y 6 de la RFC 3647
[37] Atiende a la Sección 4.6.4 y 6 de la RFC 3647

7.4.3. Otros Aspectos de los Datos de Activación

Bloqueo del dispositivo o cuenta tras intentos fallidos.

7.5. Controles de Seguridad Informática[38]

7.5.1 Requisitos Técnicos específicos de Seguridad Informática

La información del sistema de DICERT AC está protegida contra accesos no autorizados a través de una combinación de controles del sistema operativo, físicos y de redes. Se hace uso de AWS IAM, hardening de instancias EC2 y monitoreo con Amazon GuardDuty. Los controles de seguridad de redes se especifican en la ***Sección 7.7***.

Los sistemas de la AC utilizan autenticación de doble factor para todas las cuentas con capacidad de afectar directamente la emisión de certificados.

7.5.2. Clasificación de Seguridad Informática

DICERT cuenta con una ***Política de Clasificación de la Información*** que establece: La información debe ser clasificada respecto de su confidencialidad, para ello se consideran los siguientes niveles de clasificación:

a. **Confidencial (Alta):** La información está restringida para ser conocida solamente por un ámbito de personas acotado al interior de la empresa, el acceso está limitado a las personas y a las acciones definidas.
b. **Uso Interno (Media):** La información no tiene restricciones para ser conocida al interior de la empresa, todos los empleados podrían acceder a ella, si esto es necesario para el correcto desempeño de sus funciones.
c. **Público (Baja):** La información no tiene restricciones para su divulgación en todo ámbito, tanto interno como externo.

7.6. Controles Técnicos del Ciclo de Vida[39]

7.6.1. Controles de Sistema de Desarrollo

DICERT utiliza software que ha sido probado formalmente para determinar su idoneidad y aptitud para el propósito que se le da. El hardware y acceso a redes es tercerizado a proveedores líderes en la industria con capacidad de cumplir los estándares operativos y de seguridad exigidos por DICERT.

Los entornos de desarrollo, pruebas y producción se encuentran segregados.

[38] Atiende a la Sección 4.6.5 y 6 de la RFC 3647
[39] Atiende a la Sección 4.6.6. y 6 de la RFC 3647

7.6.2. Controles de Gestión de Seguridad

DICERT ha establecido una Unidad de Seguridad de la Información que implementa y opera marcos de trabajo de control interno y abarca medidas de nivel técnico, organizacional y de procedimientos. En cuanto a la protección de datos personales, DICERT ha identificado un Delegado de Protección de Datos, de conformidad con la legislación local.

7.6.3. Controles de Seguridad de Ciclo de Vida

La gestión de seguridad del sistema se controla a través de los privilegios asignados a las cuentas de la infraestructura de la AC y mediante los Roles de Confianza descritos en esta DPC.

7.7. Controles de Seguridad de Red[40]

Los equipos seguros en los cuales operan las AC de DICERT se encuentran detrás de dispositivos de firewall, en conjunto con definiciones de VPC, que restringen el acceso sólo a la red interna de DICERT y sólo a los puertos utilizados para administrar la AC y emitir Certificados.

7.8. Sellado de Tiempo[41]

7.8.1 Protocolos y Estándares de Sellado de Tiempo

DICERT opera una Autoridad de Sellado de Tiempo (TSA) que cumple estrictamente con el protocolo definido en la **RFC 3161** (*Internet X.509 Public Key Infrastructure Time-Stamp Protocol*) y los requisitos de seguridad de la norma **ETSI EN 319 421**. Los sellos de tiempo generados garantizan la integridad de los datos y la existencia de los mismos en un momento determinado.

7.8.2 Precisión y Sincronización del Reloj

La precisión del reloj de la TSA se mantiene dentro de un margen de error máximo de **un (1) segundo** respecto a la hora UTC (Coordinated Universal Time). Para asegurar esta precisión, DICERT utiliza:

- **Fuentes de Tiempo:** Sincronización redundante mediante el servicio *Amazon Time Sync Service*, el cual utiliza una flota de relojes atómicos y satélites GPS en la infraestructura de AWS.
- **Monitoreo:** Sistemas de alerta automatizados que detectan cualquier deriva (drift) superior al umbral permitido, bloqueando la emisión de sellos de tiempo si se pierde la sincronización de confianza.

[40] Atiende a la Sección 4.6.7. y 6 de la RFC 3647
[41] Atiende a la Sección 4.6.8. y 6 de la RFC 3647; y RFC 3161

7.8.3 Protección Criptográfica del Servicio de Sellado de Tiempo

Las claves privadas de la TSA se generan, almacenan y operan exclusivamente dentro de los módulos de seguridad de hardware (**AWS CloudHSM**) con certificación **FIPS 140-2 Nivel 3**. Se prohíbe explícitamente la exportación de estas claves en texto plano. Cada sello de tiempo emitido es firmado digitalmente por la clave privada de la TSA, asegurando el no repudio del origen y del tiempo.

7.8.4 Formato y Contenido del Sello de Tiempo

Cada respuesta de sellado de tiempo (TST) incluye, al menos:

1. El identificador del algoritmo de hash utilizado (SHA-256 o superior).
2. El valor del hash de los datos sellados.
3. El número de serie único del sello de tiempo.
4. La fecha y hora UTC certificada.
5. La firma digital de la TSA de DICERT.

7.8.5 Disponibilidad y Registro de Sellos de Tiempo:

El servicio de sellado de tiempo está diseñado para alta disponibilidad (99.9%) mediante el despliegue en múltiples zonas de disponibilidad de AWS. Todos los sellos de tiempo emitidos se registran y archivan de forma inmutable por un periodo de **10 años**, permitiendo verificaciones posteriores incluso si el certificado de la TSA ha expirado o ha sido revocado.

8. Perfiles de Certificados, CRL y OCSP[42]

8.1. Perfil del Certificado[43]

Los certificados de DICERT cumplen con el RFC 5280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Las extensiones de certificado y su criticidad, así como los identificadores de objetos del algoritmo criptográfico, se completan de acuerdo con los estándares IETF RFC 5280.

8.1.1. Número de Versión

Los Certificados de Suscriptores emitidos por las AC de DICERT cumplen la versión 3 de X.509.

[42] Atiende a la Sección 4.7. y 6 de la RFC 3647 y norma técnica ARCOTEL-2024-0176: Art. 5, Numeral 1, o)
[43] Atiende a la Sección 4.7.1. y 6 de la RFC 3647

8.1.2. Extensiones de los certificados

Los campos y extensiones de los certificados se establecerán de acuerdo con RFC 5280. Las extensiones que se pueden incluir son:

- Authority Key Identifier
- Subject Key Identifier
- Key Usage
- Certificate Policies
- Subject Alt Name
- Extended Key Usage
- CRL Distribution Points
- Authority Information Access
- Basic Constraints

La definición específica para cada tipo de Certificado se establece en la Política de Certificados respectiva.

8.1.3. Identificación de Objeto del Algoritmo

Se utilizan las siguientes identificaciones de objetos (OIDs):

- OID del algoritmo de firma Sha256 con encriptación RSA.
- OID del algoritmo de clave pública RSA Encryption.

8.1.4. Formas de los Nombres

Al emitir un Certificado, DICERT declara que siguió el procedimiento establecido en esta DPC para verificar que, a partir de la fecha de emisión, la información de los campos: *Surname, Given Name, Common Name (CN)* son correctos y corresponden al nombre distintivo del Suscriptor y cumple con las estipulaciones descritas en la ***Sección 4.2.***

Los campos de *Surname, Given Name, Common Name (CN)* siempre contienen información que ha sido verificada.

8.1.5. Restricciones de nombres

DICERT no impone restricciones de nombres adicionales a las definidas por el estándar X.500, asegurando que no existan espacios en blanco o caracteres no permitidos que afecten la interoperabilidad.

8.1.6. Identificador de objeto de la política de certificados

Los Certificados de Suscriptores podrán incluir los siguientes identificadores de objetos confirmando su cumplimiento con esta DPC y para indicar qué método de validación fue usado para su emisión.

Los OIDs correspondientes a esta DPC son:

a) Certificado Persona natural: 1.3.6.1.4.1.62486.2.1.1
b) Certificado de Miembro de Empresa o empleado con relación de dependencia: 1.3.6.1.4.1.62486.2.2.1
c) Certificado de Representante Legal: 1.3.6.1.4.1.62486.2.3.1
d) Certificado de Sello Electrónico: 1.3.6.1.4.1.62486.2.4.1
e) Certificado de Sellado de Tiempo: 1.3.6.1.4.1.62486.2.5.1
f) Certificado de Validación OSCP: 1.3.6.1.4.1.62486.2.6.1

Cada política podrá tener asignado un OID a partir de la raíz 62486.

8.1.7. Uso de la extensión de Restricciones de Políticas

DICERT no ha establecido restricciones de políticas en las extensiones de certificado.

8.1.8. Sintaxis y semántica de calificadores de política

No estipulado.

8.1.9. Semántica de procesamiento para la extensión crítica de Política de Certificados

La extensión de políticas se marca como **no crítica**, permitiendo que las aplicaciones procesen el certificado incluso si no reconocen el OID específico, siempre que validen la cadena de confianza.

8.2. Perfil CRL[44]

Un perfil de CRL (Certificate Revocation List) es un conjunto de directrices y formatos que define cómo se debe estructurar y gestionar una lista de certificados revocados. Esta lista es crucial para la seguridad de los sistemas que utilizan certificados digitales.

Las CRL emitidas por las ACs de DICERT cumplen con los estándares de RFC 5280.

8.2.1. Número de versión

DICERT soporta desde CRLs X.509 Versión 2.

8.2.2. Extensiones de CRL

No estipulado.

[44] Atiende a la Sección 4.7.2. y 6 de la RFC 3647

8.3. Perfil OCSP[45]

Todas las AC de DICERT soportan OCSP y sus servidores correspondientes cumplen con el estándar RFC 6960, que actualiza al RFC 2560.

8.3.1. Número de versión

DICERT cumple con la versión 3 de X.509.

8.3.2. Extensiones OCSP

Se utilizan las siguientes extensiones conforme al estándar X.509 versión 3:

- keyUsage: crítica
- basicContraints: crítica

9. Auditorías de Cumplimiento y Otras Evaluaciones[46]

9.1. Frecuencia y Circunstancia de la evaluación

DICERT efectúa auditorías de cumplimiento realizadas por terceros de forma anual. Adicionalmente, se reserva el derecho de llevar a cabo auditorías internas cuando lo considere necesario, ya sea como parte de su ciclo de control continuo o ante indicios de posibles fallos en el cumplimiento de sus controles de seguridad.

9.2. Identidad y Calificaciones del Evaluador

Las auditorías externas deben ser ejecutadas por entidades especializadas independientes, que cuenten con trayectoria comprobada en materia de seguridad de la información o por consultores certificados con experiencia en tecnologías de la información y ciberseguridad.

9.3. Relación del Evaluador con la Entidad Evaluada

Las auditorías por parte de terceros deben ser llevadas a cabo exclusivamente por organizaciones que no tengan vínculos directos con DICERT, ni intereses que puedan comprometer su imparcialidad.

Para las Autoridades de Registro (AR), DICERT podrá designar a su auditor interno como responsable del proceso de revisión.

9.4. Temas cubiertos en la Evaluación

Las auditorías dirigidas a las Autoridades Certificadoras (AC) de DICERT comprenden la verificación del cumplimiento de los controles definidos en esta DPC, así como la conformidad con los estándares

[45] Atiende a la Sección 4.7.3. y 6 de la RFC 3647
[46] Atiende a la Sección 4.8. de la RFC 3647 y la norma técnica ARCOTEL-2024-0176: Art. 5, Numeral 1, p)

y normativas aplicables. Estas evaluaciones se centran en garantizar la integridad operativa y normativa de los procesos de emisión y gestión de certificados.

9.5. Acciones a tomar como Resultado de Deficiencias

En caso de identificarse desviaciones o debilidades significativas durante una auditoría, se establecerán acciones correctivas que deberán ser implementadas por los responsables de la AC involucrada. Estas acciones se definirán con la participación del auditor y deberán ser aplicadas en un plazo razonable desde el momento de su notificación.

9.6. Comunicación de resultados

El informe de auditoría debe ser remitido a DICERT en un plazo no mayor a 15 días hábiles posteriores a la ejecución de la auditoría.

El documento debe detallar expresamente que el proceso evaluó los sistemas, procedimientos y operaciones relevantes asociados a la emisión de certificados electrónicos por parte de las ACs de DICERT.

10. Otros Asuntos Comerciales y Legales[47]

10.1. Tarifas

El Solicitante deberá pagar las tarifas correspondientes a los certificados solicitados, las cuales cubren exclusivamente todas las actividades que DICERT realiza para gestionar el ciclo de vida del certificado de firma electrónica contratado.

Las tarifas para personas naturales se encuentran permanentemente publicadas y disponibles en https://www.dicert.com.ec.

10.1.1 Tarifas de Emisión o Renovación de Certificados

DICERT puede establecer una tarifa por la emisión o por la renovación de los certificados, la que se informará oportunamente a los Titulares. DICERT nunca cobrará por la revocación de certificados que haya emitido.

[47] Atiende a la Sección 4.9. de la RFC 3647 y la norma técnica ARCOTEL-2024-0176: Art. 5, Numeral 1, q), s)

10.1.2. Tarifas de Acceso a Certificados

DICERT se reserva el derecho de aplicar un cargo razonable por el acceso a su base de datos de certificados, siempre que dicho acceso no contravenga lo estipulado en esta Declaración de Prácticas de Certificación.

10.1.3. Tarifas de Acceso a Información de Revocación y Estatus

El acceso a las Listas de Certificados Revocados (CRL) es gratuito, en conformidad con lo establecido en esta DPC, que exige su disponibilidad constante en el repositorio para los terceros que confían. Sin embargo, DICERT podrá establecer tarifas para la provisión de servicios personalizados relacionados con la información de estado y revocación, tales como versiones específicas de CRL, consultas OCSP bajo demanda o servicios adicionales que representen un valor agregado.

No está permitido que terceros accedan o utilicen la información de estado de certificados, CRL u OCSP contenida en los repositorios de DICERT para integrarla en productos o servicios comerciales, sin autorización expresa y por escrito de DICERT.

10.1.4. Tarifas para Otros Servicios

Servicios como sellado de tiempo o validación masiva se rigen por contratos específicos.

10.1.5. Políticas de reembolso

Según lo estipulado en la Ley Orgánica de Defensa al Consumidor, el derecho de retracto no procede, dado que los certificados son productos elaborados por la AUTORIDAD DE CERTIFICACIÓN conforme a las especificaciones proporcionadas por el Titular (nombre, RUC y correo electrónico). La negativa posterior a aceptar un certificado por motivos distintos a errores o inexactitudes en el mismo, o la no utilización del certificado, no confiere al Titular el derecho a solicitar un reembolso.

Se establece una política de reembolso limitada a errores técnicos imputables a la AC dentro de los primeros 5 días de emisión.

10.2. Responsabilidad Financiera[48]

10.2.1. Cobertura de Seguros

De conformidad con la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su reglamento, DICERT mantiene una póliza general de responsabilidad civil adecuada, garantizando así una cobertura suficiente de su responsabilidad.

Esta póliza no cubre actos relacionados con el incumplimiento de las obligaciones contraídas por el Suscriptor o el uso incorrecto de un Certificado y/o sus llaves privadas.

[48] Atiende a la Sección 4.9.2. y 6 de la RFC 3647

10.2.2. Otros activos

La entidad garantiza su continuidad operativa con activos propios y respaldo tecnológico en AWS.

10.2.3. Cobertura de seguro o garantía para las entidades finales

No se ofrece un seguro de garantía individual a menos que se pacte en contratos corporativos específicos.

10.3. Confidencialidad de la Información Empresarial[49]

10.3.1. Alcance de la Confidencialidad de Información

La siguiente información relacionada con el Solicitante y el Suscriptor se considera información confidencial:

1. Solicitudes de certificados, aprobadas o rechazadas;
2. Registros presentados por el solicitante en apoyo de las solicitudes de certificado;
3. Claves privadas;
4. Archivos de registro y otros registros de auditoría;
5. Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
6. Planes de continuidad de negocio y recuperación de desastres.
7. Planes de seguridad.
8. Documentación de operaciones, archivo, monitorización y otros análogos.
9. Toda otra información identificada como “Confidencial”.

10.3.2. Información No Confidencial

Los certificados y los datos de revocación no se consideran información confidencial, así como tampoco las listas de revocación de certificados (CRL’s), y las restantes informaciones de estado de revocación. La información contenida en el registro público de certificados (OCSP). Cualquier información cuya publicidad sea impuesta normativamente o de conformidad con esta DPC, y en general, toda otra información que no esté identificada como “Uso Interno” o “Confidencial”.

10.3.3. Responsabilidad de Proteger la Información Confidencial

DICERT, sus contratistas y agentes utilizan medidas razonables de cuidado cuando procesan y al proteger información confidencial. Al respecto, DICERT incorpora cláusulas de confidencialidad en los contratos que mantiene con sus proveedores, contratistas, agentes y dependientes.

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

[49] Atiende a la Sección 4.9.3. y 6 de la RFC 3647

10.4. Privacidad de la Información Personal[50]

10.4.1. Plan de Privacidad

Para DICERT, la privacidad de la información es fundamental y con el objetivo de protegerla adecuadamente, hemos desarrollado una ***Política de Privacidad y Protección de Datos Personales***, la que detalla cómo gestionamos los datos personales de los Titulares de certificados de firmas, cumpliendo con el marco legal establecido por la Ley Orgánica de Protección de Datos Personales. Puede consultar nuestra política vigente en https://www.dicert.com.ec.

10.4.2. Información que se trata como Privada

Los datos personales que DICERT trata son antecedentes personales, antecedentes demográficos, biométricos y datos recolectados a través de tecnologías de cookies a través de su sitio Web.

Cualquier información sobre los Titulares que no está disponible públicamente a través del contenido del Certificado emitido, el directorio de Certificados y la CRL en línea se trata como información privada.

10.4.3. Información no privada

Ver Sección 10.4.1. y 10.4.2.

10.4.4. Responsabilidad para proteger información privada

Ver Sección 10.4.1. Además. se hace uso de cifrado AES-256 para el almacenamiento de datos personales en AWS S3.

10.4.5. Aviso y Consentimiento de Uso de Información Privada

Ver Sección 10.4.1. Además, el suscriptor autoriza el tratamiento de datos mediante la firma del formulario de solicitud.

10.4.6. Divulgación de Conformidad con Procesos Judiciales o Administrativos

Ver Sección 10.4.1. Además, se declara que DICERT entregará información únicamente bajo orden de autoridad competente.

10.4.7. Otras circunstancias de divulgación de información

Ninguna otra fuera de las legales.

[50] Atiende a la Sección 4.9.4. y 6 de la RFC 3647

10.5. Derechos de Propiedad Intelectual[51]

DICERT, o sus otorgantes de licencias, poseen los derechos de propiedad intelectual de los servicios de DICERT AC, incluidos los Certificados, las marcas comerciales utilizadas para proporcionar servicios de Certificados y esta DPC.

La información del certificado y la revocación son propiedad exclusiva de DICERT. DICERT otorga permiso para reproducir y distribuir certificados de forma no exclusiva y libre de regalías, siempre que se reproduzcan y distribuyan en su totalidad. DICERT no permite trabajos derivados de sus Certificados o productos sin un permiso previo por escrito.

Las claves privadas y públicas siguen siendo propiedad de los suscriptores que las poseen legítimamente. Todos los recursos compartidos secretos (elementos distribuidos) de las claves privadas de DICERT son propiedad de DICERT.

10.6. Representaciones y Garantías[52]

10.6.1. Representaciones y Garantías de la AC

DICERT ofrece la siguiente garantía limitada a los Beneficiarios del Certificado en el momento de la emisión del Certificado:

a) Se emitió el Certificado sustancialmente de conformidad con esta DPC;
b) La información contenida en el Certificado refleja con precisión la información proporcionada a DICERT por el Solicitante en todos los aspectos materiales; y
c) Ha tomado medidas razonables para verificar que la información contenida en el Certificado sea precisa.

Los pasos que DICERT da para verificar la información contenida en un Certificado se establecen en esta DPC.

Sin perjuicio de las demás obligaciones que impone la ley, respecto de un suscriptor, DICERT se compromete especialmente a:

a. Ofrecer y mantener las instalaciones, sistemas, programas informáticos y recursos humanos necesarios para otorgar Certificados Electrónicos conforme la normativa vigente.
b. Cumplir con los procedimientos establecidos en ésta DPC.
c. Comprobar la identidad del solicitante de un certificado de firma electrónica según los procedimientos establecidos.

[51] Atiende a la Sección 4.9.5. y 6 de la RFC 3647
[52] Atiende a la Sección 4.9.6. de la RFC 3647 y norma técnica ARCOTEL-2024-0176: Art. 5, Numeral 1, e), f), r)

d. Aprobar o rechazar las solicitudes de certificados, directamente o a través de las Autoridades de Registro, de conformidad con ésta DPC.
e. Brindar soporte cuando lo requiera el titular.
f. Cumplir con las disposiciones de la Ley de Defensa del Consumidor, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Norma Técnica ARCOTEL-2024-0176; la Ley Orgánica de Protección de Datos Personales; y reglamentos respectivos.
g. Mantener un registro público de certificados emitidos y aquellos que han quedado sin efecto en la página web de DICERT, y comunicar cualquier hecho que pudiera afectar la validez de los certificados.

10.6.2. Representaciones y Garantías de la AR

La Autoridad de Registro se compromete a:

a) Comprobar la identidad del solicitante de un certificado electrónico, según el procedimiento establecido en esta DPC.
b) Obtener la aceptación del contrato del Titular por parte del solicitante.
c) Aprobar o rechazar las solicitudes de certificados, directamente o a través de sus Entidades de Registro, conforme a las DPC.
d) Permitir operar solo certificados de firma electrónica avanzada que hayan sido aceptados por el solicitante.
e) Conservar por 10 años la información utilizada como base para la emisión de los certificados electrónicos o remitir a DICERT dentro de los plazos convenidos.
f) Recibir las solicitudes de revocación de certificados e informarlas a DICERT.
g) Prestar cualquier otro servicio que DICERT le solicite y que guarde relación con la actividad de certificación electrónica.

La Autoridad de Registro realiza todas las actuaciones indicadas anteriormente, gestionando el ciclo de vida del certificado de firma electrónica avanzada, por cuenta y riesgo de DICERT.

10.6.3. Representaciones y Garantías del Suscriptor

DICERT requiere, como parte del Contrato o Acuerdo de Términos de Uso, que el Solicitante asuma los compromisos y garantías de esta Sección en beneficio de la AC y los Beneficiarios del Certificado.

Antes de la emisión de un Certificado, DICERT obtiene, para su beneficio expreso y el de los Beneficiarios del Certificado, ya sea:

1. La aceptación por parte del Solicitante del Contrato con la AC, o
2. La aceptación por parte del Solicitante del Acuerdo de Términos de Uso.

DICERT implementa un proceso para garantizar que cada Contrato o Acuerdo de Términos de Uso sea legalmente exigible contra el Solicitante. En cualquier caso, el Contrato debe aplicarse al Certificado

que se emitirá de conformidad con la solicitud del certificado. DICERT puede usar un contrato electrónico o de "clic" a condición de que haya determinado que dichos acuerdos son legalmente exigibles. Se puede usar un Acuerdo separado para cada solicitud de certificado, o un solo Acuerdo para cubrir múltiples solicitudes de certificados futuras y los Certificados resultantes, siempre que cada Certificado que la AC emita al Solicitante esté claramente cubierto por un documento legal aceptado entre las partes.

El Contrato o Acuerdo de Términos de Uso contiene disposiciones que imponen al Solicitante o su representada las siguientes obligaciones y garantías:

1. **Exactitud de la información**: Obligación y garantía de proporcionar información precisa y completa en todo momento a DICERT, tanto en la solicitud del certificado como en la solicitud de DICERT en relación con la emisión de los Certificados que se proporcionarán;
2. **Protección de la clave privada**: Obligación y garantía del solicitante de tomar todas las medidas razonables para mantener el control exclusivo, mantener la confidencialidad y proteger adecuadamente en todo momento la clave privada que corresponde a la clave pública que se incluirá en el certificado solicitado (y cualquier dispositivo o datos de activación asociados, por ejemplo, contraseña o token);
3. **Aceptación del Certificado**: Obligación y garantía que el Suscriptor revisará y verificará la exactitud del contenido del Certificado;
4. **Uso del Certificado**: Obligación y garantía de utilizar el Certificado únicamente de conformidad con todas las leyes aplicables y de acuerdo con el Contrato y Acuerdo de Términos de Uso;
5. **Informes y revocación**: Obligación y garantía de dejar de usar rápidamente un Certificado y su Clave privada asociada, y solicitar de inmediato a DICERT que revoque el Certificado, en caso de que:
    a) Cualquier información en el Certificado sea incorrecta o se vuelva incorrecta o inexacta, o
    b) Exista un uso indebido o divulgación real o sospecha de la que clave privada del suscriptor asociada con la clave pública incluida en el certificado ha sido comprometida;
6. **Terminación del uso del certificado**: Obligación y garantía de suspender rápidamente el uso de la clave privada correspondiente a la clave pública incluida en el certificado tras la revocación de dicho certificado por razones de compromiso o divulgación de la clave.
7. **Capacidad de respuesta**: Obligación de responder a las instrucciones de DICERT sobre el uso de la clave del Certificado o el uso indebido del Certificado dentro de un período de tiempo específico.
8. **Reconocimiento y aceptación**: un reconocimiento y aceptación de que DICERT tiene derecho a revocar el certificado de inmediato si el Solicitante viola los términos del Contrato o el Acuerdo de Términos de Uso o si DICERT descubre que el Certificado se está utilizando para actividades ilegales.

Los Contratos y el Acuerdo de Términos de Uso pueden incluir representaciones y garantías adicionales.

10.6.4. Representaciones y Garantías de los Terceros que Confían

Los Terceros que Confían declaran y garantizan que:

a) Han leído, entienden y aceptan esta DPC;
b) Han verificado tanto el Certificado de DICERT AC, como cualquier otro certificado en la cadena de certificados utilizando la CRL u OCSP pertinente;
c) No utilizarán un Certificado si el Certificado ha expirado o ha sido revocado;
d) Tienen información suficiente para tomar una decisión informada sobre el grado en que eligen confiar en la información en un Certificado;
e) Han estudiado las limitaciones aplicables en el uso de Certificados y están de acuerdo con las limitaciones de DICERT sobre la responsabilidad relacionada con el uso de Certificados;
f) Son los únicos responsables de decidir si confiar o no en la información contenida en un Certificado; y
g) Son los únicos responsables de las consecuencias legales y de otro tipo de su incumplimiento de las obligaciones de la Parte Confiable en esta DPC.

Los Terceros que Confían también declaran y garantizan que tomarán todas las medidas razonables para minimizar el riesgo asociado con confiar en un certificado electrónico, incluyendo solo confiar en un Certificado después de considerar:

1. La ley aplicable y los requisitos legales para la identificación de una parte, la protección de la confidencialidad o privacidad de la información y la exigibilidad de la transacción;
2. El uso previsto del Certificado como se indica en el Certificado o en esta DPC;
3. Los datos enumerados en el Certificado;
4. El valor económico de la transacción o comunicación;
5. La pérdida o daño potencial que sería causado por una identificación errónea o una pérdida de confidencialidad o privacidad de la información en la aplicación, transacción o comunicación;
6. La experiencia previa del Tercero que Confía lidiando con el Suscriptor.
7. La opinión y experiencia del Tercero que Confía respecto de los métodos de comercio basados en computadora; y
8. Cualquier otro indicio de confiabilidad o falta de confiabilidad perteneciente al Suscriptor y / o la aplicación, comunicación o transacción.

10.6.5. Representaciones y Garantías de Otros Participantes

Aplicables según contratos específicos.

10.7. Exclusión de Garantías[53]

DICERT no se hará responsable en las siguientes circunstancias respecto de la emisión y uso de los Certificados emitidos:

a. Desastres naturales o cualquier otro caso de fuerza mayor.
b. Uso de los certificados fuera del cumplimiento de esta DPC, fuera de su período de vigencia o cuando hayan sido revocados.
c. Uso fraudulento de los Certificados, CRL o cualquier otra información relacionada.
d. Por daños y/o prejuicios producto de la interpretación errada de esta Declaración de Prácticas de Certificación por parte de los Participantes.
e. Por el incumplimiento de las obligaciones del Contrato suscrito con el usuario, Términos de Servicio o la ley vigente.
f. Por el contenido de los mensajes, sitios web o documentos firmados y/o cifrados usando los Certificados.
g. Por fraudes en la documentación presentada por el Solicitante.

10.8. Limitación de Responsabilidad[54]

DICERT será responsable hasta de culpa leve y responderá por los daños y perjuicios que cause a cualquier persona natural o jurídica, en el ejercicio de su actividad, cuando DICERT incumpla las obligaciones que le impone la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos o actúe con negligencia, sin perjuicio de las sanciones previstas en la Ley Orgánica de Defensa del Consumidor.

DICERT no asume ninguna responsabilidad por firmas, certificados, o cualquier otro servicio o documento relacionado, que sean usados de manera incorrecta o para fines ilícitos, o para aquellos fines que excedan los límites de buen uso contemplados en el contrato suscrito con el usuario, en el certificado, en Acuerdo de Términos de Uso o la Declaración de Prácticas de Certificación de DICERT.

10.9. Indemnizaciones[55]

En concordancia con el artículo 30 literal h) de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, DICERT establece una **garantía de responsabilidad** con la finalidad de asegurar a los usuarios el pago de daños y perjuicios como resultado por el incumplimiento culpable de sus obligaciones, conforme los siguientes parámetros:

a. En el evento de incumplimiento de obligaciones DICERT asumirá hasta un valor equivalente al 100% del precio pagado por el suscriptor por la firma electrónica contratada.

[53] Atiende a la Sección 4.9.7. y 6 de la RFC 3647
[54] Atiende a la Sección 4.9.8. y 6 de la RFC 3647 y norma técnica ARCOTEL-2024-0176: Art. 5, Numeral 1, d), r)
[55] Atiende a la Sección 4.9.9. y 6 de la RFC 3647

b. Conforme lo establecido por el Reglamento a la Ley de Comercio Electrónico, para la ejecución de la garantía el procedimiento consistirá en que el usuario presente a la autoridad nacional competente (ARCOTEL al momento de suscripción de este contrato), una solicitud motivada en el término de 15 días a partir de que se produjo el supuesto incumplimiento culpable, para que al amparo de lo dispuesto en el artículo 31 de la Ley mencionada, ésta ponga en conocimiento de DICERT el reclamo formulado.
c. A partir de la comunicación recibida, DICERT tendrá 5 días término para presentar sus descargos, resolver dicho reclamo o reconocer el incumplimiento.
d. Una vez fenecido el término antes referido, dentro del término de 5 días posteriores la autoridad nacional competente deberá resolver sobre la procedencia del reclamo formulado, y de ser el caso ordenar la ejecución parcial de la garantía de responsabilidad por el monto de los daños y perjuicios causados y debidamente probados, los que no podrán reconocerse por un valor superior al pactado en este contrato y que son de un valor equivalente al 100% del precio pagado por el Usuario por la certificación electrónica contratada. Sin perjuicio de lo anterior, el usuario podrá considerar el inicio de las acciones que estime pertinentes en contra de la Entidad de Certificación de Información y Servicios Relacionados, por los daños y perjuicios no cubiertos por la garantía de responsabilidad.
e. En cualquier caso, el usuario tiene la obligación de probar de manera adecuada y objetiva el daño sufrido, así como su relación de causalidad con el supuesto incumplimiento culpable.

Por su parte, el suscriptor se obliga a indemnizar a DICERT por cualquier daño derivado de la falsedad en sus datos o el compromiso de su clave por descuido.

10.10. Vigencia y Terminación[56]

10.10.1. Plazo

Esta DPC entra en vigencia al momento de su publicación en el Repositorio. Las enmiendas a esta DPC entrarán en vigencia al momento de su publicación en el Repositorio.

10.10.2. Terminación

Esta DPC y cualquier enmienda se mantienen vigentes hasta que sean reemplazadas por una nueva versión.

10.10.3. Efectos de la Terminación y supervivencia

A la terminación de esta DPC, los participantes están sujetos a sus términos para todos los certificados emitidos por el resto de los períodos de validez de dichos certificados. Las cláusulas de confidencialidad y responsabilidad sobreviven a la terminación del documento.

[56] Atiende a la Sección 4.9.10. y 6 de la RFC 3647

10.11. Notificaciones y Comunicaciones Individuales con los Participantes[57]

A menos que se especifique lo contrario por acuerdo entre las partes, los Participantes utilizarán métodos comercialmente razonables, de preferencia los correos electrónicos identificados en los contratos suscritos, para comunicarse entre sí; y a través de notificaciones en el portal de DICERT.

10.12. Enmiendas[58]

10.12.1. Procedimiento para Enmiendas

DICERT puede cambiar esta DPC en cualquier momento a su exclusivo criterio y sin previo aviso a los Suscriptores o Terceros que Confían. La DPC y sus enmiendas están disponibles en el Repositorio.

Cualquier enmienda a esta DPC se evidenciará con un nuevo número de versión y fecha, previa la presentación a la ARCOTEL.

10.12.2. Mecanismos de Notificación y Período

DICERT puede proporcionar un aviso adicional (en el Repositorio o en un sitio web separado) en caso de que realice cambios importantes en su DPC. DICERT es responsable de determinar qué constituye un cambio importante de la DPC. DICERT no garantiza ni establece un período de notificación para los Suscriptores.

Todas las enmiendas a la DPC serán notificadas a la Entidad de Control respectiva según lo requiera la Ley.

10.12.3 Circunstancias en las que debe cambiar el OID

Si DICERT determina que es necesario realizar un cambio en el identificador de objeto (OID) correspondiente a la Declaración de Prácticas de Certificación, la enmienda deberá incluir los nuevos identificadores de objeto (OID) de dicha DPC.

10.13. Disposiciones de Resolución de Disputas[59]

Toda cuestión, diferencia o controversia derivada o relacionada con el contrato suscrito con el usuario, cuando no se llegase a un acuerdo amigable directo, deberá ser sometida a un **proceso de mediación ante el Centro de Arbitraje y Mediación (CAM) de la Cámara de Comercio de Quito**, y de no darse un acuerdo, cualquier diferencia será resuelta mediante arbitraje administrado y confidencial por el mismo Centro de Arbitraje y Mediación (CAM) de la Cámara de Comercio de

[57] Atiende a la Sección 4.9.11. y 6 de la RFC 3647
[58] Atiende a la Sección 4.9.12. y 6 de la RFC 3647
[59] Atiende a la Sección 4.9.13. y 6 de la RFC 3647

Quito; siguiendo para el efecto lo previsto en la Ley de Arbitraje y Mediación y el Reglamento del referido CAM.

10.14. Ley Aplicable[60]

La operación de DICERT AC y esta DPC, así como las Políticas de Certificados están sujetos a la siguiente normativa:

1. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el suplemento del Registro Oficial No. 577 de fecha 17 de abril de 2002. [Ley No. 2002 –67].
2. Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (No. 3496) y las Reformas contenidas en los decretos 1356 y 867.
3. Norma Técnica ARCOTEL-2024-0176 de 16 de agosto de 2024, publicada en el Registro Oficial, Cuarto Suplemento Nº 640 del 10 de septiembre de 2024.

10.15. Cumplimiento de la Ley Aplicable[61]

Esta DPC está sujeta a las leyes, normas, reglamentos, ordenanzas, decretos y resoluciones emitidas por las autoridades de control de la República del Ecuador, relacionadas con la materia, pero no limitando a: comercio electrónico, firmas electrónicas y mensajes de datos; defensa del consumidor; protección de datos personales, propiedad intelectual, comercial, civil y penal.

10.16. Disposiciones varias[62]

10.16.1. Acuerdo Completo

Esta DPC constituye el acuerdo total de prácticas de certificación.

10.16.2. Cesión

Los Terceros que Confían y los Suscriptores no pueden asignar sus derechos u obligaciones bajo esta DPC, por ley o de otro modo, sin la aprobación previa por escrito de DICERT. Cualquier intento de asignación será nulo. Sujeto a lo anterior, esta DPC será vinculante y redundará en beneficio de las partes del presente, sus sucesores y cesionarios permitidos.

DICERT puede ceder sus derechos bajo este documento previa autorización de ARCOTEL.

[60] Atiende a la Sección 4.9.14. y 6 de la RFC 3647
[61] Atiende a la Sección 4.9.15. y 6 de la RFC 3647
[62] Atiende a la Sección 4.9.16. y 6 de la RFC 3647

10.16.3. Divisibilidad

Si alguna disposición de esta DPC se considera inválida, ilegal o inaplicable, la validez, legalidad o exigibilidad del resto de esta DPC no se verá afectada o perjudicada de ninguna manera por el presente.

10.16.4. Ejecución

DICERT puede solicitar indemnización y honorarios de abogados de la otra parte por daños, pérdidas y gastos relacionados con la conducta de esa parte. El hecho de que DICERT no haga cumplir una disposición de esta DPC no significa que renuncie al derecho de DICERT de hacer cumplir la misma disposición más adelante o del derecho de hacer cumplir cualquier otra disposición de esta DPC. Para ser efectivos, las exenciones deben ser por escrito y firmadas por DICERT.

10.16.5. Fuerza Mayor

DICERT no será responsable de ningún incumplimiento o retraso en el cumplimiento de sus obligaciones en virtud del presente documento en la medida y mientras dicho incumplimiento o retraso sea causado, directa o indirectamente, por fuego, inundación, terremoto, o elementos de la naturaleza, actos de guerra, terrorismo, disturbios, desórdenes civiles, rebeliones o revoluciones en los Estados Unidos de América (donde se mantienen los servidores que soportan la infraestructura de llave pública) o la República del Ecuador, huelgas, cierres patronales o dificultades laborales o cualquier otra causa similar más allá del control razonable de DICERT.

10.17. Otras Disposiciones

No aplica.

11. Control de Cambios

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DICERT						
CÓDIGO: DPC-DES-DC-1001					**CLASIFICACIÓN:** Documento de Acceso Público	
VERSIÓN	**DETALLE**	**ELABORADO POR:**	**FECHA APRUEBA**	**REVISADO POR:**	**FECHA PUBLICACIÓN**	**LOCALIZACIÓN**
1.0	Versión Inicial	Paúl Quiñonez	08/04/2025	Galo Becerra	04/04/2025	https://dicert.com.ec/links/dpc
2.0	Revisión ARCOTEL	Paúl Quiñonez	19/01/2026	Galo Becerra	22/01/2026	https://dicert.com.ec/links/dpc