Declaración de Prácticas de Certificación (DPC)

Entidad de Certificación de Información

DARKCAM S.A.

Plataforma de Servicios: **Universe-ID**

Versión:	3.0
Fecha de Entrada en Vigor:	14 de Agosto del 2026

Tabla de Contenido

1. INTRODUCCIÓN

1.1. Descripción General

La presente Declaración de Prácticas de Certificación (DPC) detalla las políticas, procedimientos y controles implementados por **DARKCAM S.A.**, una Entidad de Certificación de Información (ECI) acreditada por la Agencia de Regulación y Control de las Telecomunicaciones (**ARCOTEL**) de Ecuador.

DARKCAM S.A. opera la plataforma de identidad digital **Universe-ID** (https://universe-id.com), un servicio diseñado para la emisión, gestión y validación de certificados de firma electrónica de manera completamente digital y automatizada. Nuestra infraestructura se basa en una arquitectura moderna de microservicios y servicios administrados en la nube, garantizando los más altos estándares de seguridad, disponibilidad y escalabilidad.

Esta DPC se estructura conforme al estándar **IETF RFC 3647** y describe las prácticas aplicadas para la emisión de los siguientes tipos de certificados de firma electrónica en Ecuador:

- Persona Natural (con y sin RUC)
- Miembro de Empresa
- Representante Legal
- Sello Electrónico (contemplado; no comercializado a la fecha — ver Sección 9.1.1)

El documento está dirigido a suscriptores, partes de confianza y al público en general que interactúa con los certificados emitidos por DARKCAM S.A.

1.2. Nombre e Identificación del Documento

Este documento se denomina *«Declaración de Prácticas de Certificación (DPC) de DARKCAM S.A.»*. Las versiones del documento son gestionadas mediante un número de versión y la fecha de entrada en vigor, indicados en la cabecera del mismo. Cada política de certificación emitida bajo esta DPC está identificada por un Identificador de Objeto (OID) único, conforme a los estándares internacionales.

Datos de identificación de la versión vigente: Nombre: Declaración de Prácticas de Certificación (DPC) de DARKCAM S.A.; Versión: 3.0; Estado: VIGENTE; Fecha de entrada en vigor: 14 de Agosto del 2026; URL de acceso público: https://universe-id.com/darkcam/cps.pdf.

Las políticas de certificación operadas por DARKCAM S.A. se identifican bajo el arco de Identificadores de Objeto (OID) asignado a la entidad por la IANA (Private Enterprise Number): 1.3.6.1.4.1.64482. Los OID de política por tipo de certificado son los siguientes. Certificados en archivo (software), rama .2: Persona Natural (con y sin RUC) 1.3.6.1.4.1.64482.2.1.1; Miembro de Empresa 1.3.6.1.4.1.64482.2.2.1; Sello Electrónico 1.3.6.1.4.1.64482.2.2.2; Representante Legal 1.3.6.1.4.1.64482.2.3.1; Sello de Tiempo 1.3.6.1.4.1.64482.2.5.1. Certificados sobre Dispositivo Seguro de Creación de Firma (DSCF), rama .3:

Persona Natural 1.3.6.1.4.1.64482.3.1.1; Miembro de Empresa 1.3.6.1.4.1.64482.3.2.1; Sello Electrónico 1.3.6.1.4.1.64482.3.2.2; Representante Legal 1.3.6.1.4.1.64482.3.3.1. Cada OID se publica en la extensión «Políticas de Certificado» (Certificate Policies) del certificado correspondiente, junto con el localizador de esta DPC (CPS URI).

Historial de versiones.

Versión	Aprobación interna	Publicación	Estado	Principales cambios
1.0	01-10-2025	01-10-2025	Sustituida	Versión inicial
2.0	01-12-2025	01-12-2025	Sustituida	Forma de emitir los certificados
3.0	14-08-2026	14-08-2026	**Vigente**	OID por tipo de certificado, certificados short-lived, perfiles RFC 5280, secciones 5.7 y 6.4–6.7, y capítulo 9 completo

1.3. Participantes de la PKI

1.3.1. Autoridad de Certificación (AC)

DARKCAM S.A. opera una jerarquía de certificación de dos niveles, implementada sobre la plataforma **AWS Private Certificate Authority**, para asegurar la máxima protección de las claves raíz.

- **Autoridad de Certificación Raíz (Root CA):**
  - **Algoritmo:** RSA 4096 bits con SHA-256.
  - **Estado: Offline.** Su clave privada está protegida en un Módulo de Seguridad de Hardware (HSM) con certificación FIPS 140-2 Nivel 3 o superior. Se activa únicamente para firmar el certificado de la Autoridad de Certificación Subordinada.
- **Autoridad de Certificación Subordinada (SubCA DARKCAM):**
  - **Algoritmo:** RSA 4096 bits con SHA-256.
  - **Estado: Online.** Es la CA que emite, gestiona y revoca los certificados de firma electrónica para los suscriptores finales. Su clave privada está igualmente protegida en un HSM FIPS 140-2 Nivel 3 o superior.
- **Autoridad de Certificación Subordinada Short-Lived (SubCA DARKCAM Short):**
  - **Algoritmo:** RSA 4096 bits con SHA-256. Esta CA emite los certificados de corta duración (one-shot) con algoritmo de firma SHA-512.
  - **Estado: Online.** Es la CA que emite certificados de corta duración (short-lived) para escenarios de firma única (one-shot). Estos certificados tienen una validez máxima de un (1) día (24 horas), se emiten una sola vez para firmar un documento específico y no

requieren revocación tradicional debido a su naturaleza efímera. Su clave privada está protegida en un HSM FIPS 140-2 Nivel 3 o superior.

1.3.2. Autoridad de Registro (AR)

En la arquitectura de DARKCAM S.A., la función de Autoridad de Registro no es un ente manual o un departamento, sino que está completamente integrada y automatizada en la plataforma **Universe-ID**.

La plataforma actúa como AR realizando las siguientes funciones de manera programática:

1. **Recepción y Verificación de Datos:** Captura y valida la información del solicitante a través de su formulario de registro digital.
2. **2. Prueba de Vida (Liveness Detection):** Mediante un servicio de detección de vida (*Liveness Detection*) provisto por un proveedor tecnológico especializado, seleccionado conforme a los estándares técnicos y de seguridad definidos para la solución, el solicitante realiza una prueba de vida en tiempo real a través de la cámara de su dispositivo, permitiendo verificar que se trata de una persona real y que se encuentra físicamente presente durante el proceso. El servicio podrá ser implementado mediante Amazon Rekognition Face Liveness, a través de AWS Amplify, o mediante otro proveedor tecnológico equivalente que cumpla con los requisitos técnicos, de seguridad, disponibilidad y protección de datos establecidos para la solución.
3. **Validación Biométrica de Identidad:** Una vez superada la prueba de vida, la plataforma compara los datos biométricos faciales capturados contra los registros oficiales del **Registro Civil del Ecuador**, verificando que el solicitante corresponde al titular del documento de identidad presentado. Adicionalmente, se valida la correspondencia de cédula de identidad, RUC y/o datos de representación legal mediante integración API con fuentes oficiales.

Este proceso automatizado garantiza la identificación inequívoca del solicitante sin intervención humana, asegurando la integridad y celeridad del registro.

1.3.3. Suscriptor

Persona natural o jurídica, debidamente identificada a través de la plataforma Universe-ID, a nombre de quien se emite un certificado digital.

1.3.4. Partes de Confianza (Relying Parties)

Cualquier persona, entidad o sistema que confía en un certificado emitido por DARKCAM S.A. para verificar la validez de una firma electrónica.

1.3.5. Otros Participantes

- **Proveedores de Servicios Tecnológicos:** DARKCAM S.A. se apoya en proveedores líderes de servicios en la nube para operar su infraestructura:

- **Amazon Web Services (AWS):** Provee la infraestructura PKI central (AWS Private CA, HSM, S3, CloudTrail) y el servicio de verificación biométrica (AWS Amplify Face Liveness Detection).
- **Google Cloud Platform (GCP):** Aloja los microservicios de backend (emisión, firma de documentos).
- **Vercel:** Despliega la aplicación frontend de Universe-ID.
- **Supabase:** Provee la plataforma de base de datos.
- **Datadog:** Provee la plataforma de monitoreo y observabilidad centralizada.
- Proveedores de verificación biométrica.

1.4. Uso del Certificado

1.4.1. Uso Apropiado

Los certificados emitidos por DARKCAM S.A. están destinados exclusivamente para los siguientes propósitos:

- **Identificación:** Autenticar la identidad del suscriptor en transacciones digitales.
- **Integridad:** Garantizar que un documento o mensaje de datos no ha sido alterado desde que fue firmado.
- **No Repudio:** Proporcionar una prueba criptográfica de que el suscriptor firmó el documento, impidiendo que pueda negar su autoría.

1.4.2. Uso Prohibido

Se prohíbe el uso de los certificados para fines ilícitos, contrarios a la legislación ecuatoriana, o en sistemas cuyo fallo pueda poner en riesgo la vida humana o causar daños graves (ej. control de armas, sistemas de soporte vital).

La siguiente tabla detalla los usos permitidos y prohibidos de manera específica para cada tipo de certificado:

Tipo de certificado	Usos permitidos	Usos prohibidos
Persona Natural (con y sin RUC)	Firma electrónica de documentos y mensajes de datos a título personal del titular; autenticación de identidad; garantía de integridad y no repudio; protección de correo electrónico (S/MIME).	Representar a una empresa u organización; cifrado masivo de datos; firma de código; uso por persona distinta del titular; fines ilícitos o sistemas de riesgo para la vida humana.
Miembro de Empresa	Firma electrónica en el ejercicio de funciones dentro de la empresa que vincula al titular; autenticación, integridad y no repudio; protección de correo electrónico institucional.	Actuar como representante legal de la empresa; uso fuera de la relación de dependencia; cifrado masivo; firma de código; fines ilícitos o sistemas de riesgo para la vida humana.

Representante Legal	Firma electrónica en representación legal de la organización, obligando a la persona jurídica; autenticación, integridad y no repudio en actos propios de la representación.	Uso una vez cesada la representación legal; actos ajenos a la organización; cifrado masivo; firma de código; fines ilícitos o sistemas de riesgo para la vida humana.
Sello Electrónico	Sellado electrónico de documentos para identificar y vincular su origen a la persona jurídica (no a una persona natural); garantía de integridad y autenticidad de documentos institucionales.	Sustituir la firma de una persona natural; cifrado masivo; firma de código; fines ilícitos o sistemas de riesgo para la vida humana.

1.5. Administración de Políticas

1.5.1. Organización que administra el documento. La administración, revisión y aprobación de esta DPC y de las Políticas de Certificación corresponde al **Comité de Políticas de Certificación de DARKCAM S.A.**, integrado por Representante Legal, Responsable de Operaciones PKI y Asesor Legal. El Comité sesiona con periodicidad semestral y de forma extraordinaria ante cambios regulatorios, hallazgos de auditoría o incidentes de seguridad; sus decisiones constan en acta. Organización responsable: DARKCAM S.A., RUC 1793185541001, Pedro Ponce Carrasco E8-06 y Diego de Almagro, Edificio Almagro Plaza, Oficina 814, Quito – Ecuador.

1.5.2. Persona de contacto. Responsable: Pablo Aucapiña. Correo institucional: info@dark-cam.com, canal dedicado: administrativo@dark-cam.com. Teléfono: 0992989693. Dirección: Pedro Ponce Carrasco E8-06 y Diego de Almagro, Edificio Almagro Plaza, Of. 814, Quito. Horario de atención: lunes a viernes, 09h00 a 18h00 (UTC-5). Plazos de respuesta: acuse de recibo dentro de 24 horas hábiles; respuesta de fondo a consultas sobre la DPC dentro de 5 días hábiles; solicitudes de revocación por compromiso de clave: atención inmediata, disponible 24/7 en el portal de autogestión.

1.6. Definiciones y Acrónimos

Término	Definición
ARCOTEL	Agencia de Regulación y Control de las Telecomunicaciones de Ecuador.
CA	Autoridad de Certificación (Certificate Authority).
CRL	Lista de Revocación de Certificados (Certificate Revocation List).
DPC	Declaración de Prácticas de Certificación.
ECI	Entidad de Certificación de Información.
FIPS	Federal Information Processing Standards.
HSM	Módulo de Seguridad de Hardware (Hardware Security Module).
OCSP	Protocolo de Estado de Certificados en Línea (Online Certificate Status Protocol).

PKI	Infraestructura de Clave Pública (Public Key Infrastructure).
Google Cloud Run	Plataforma serverless para la ejecución de microservicios.
Supabase	Plataforma de base de datos como servicio.
Vercel	Plataforma de despliegue para aplicaciones frontend.

2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO

2.1. Repositorios

DARKCAM S.A. mantiene repositorios públicos y de libre acceso para que las partes de confianza puedan verificar la validez y el estado de los certificados.

- **Certificado de la SubCA DARKCAM:** Se encuentra en el sitio web de DARKCAM (www.universe-id.com).
- **Lista de Revocación de Certificados (CRL):** La URL de la CRL se encuentra embebida en la extensión «Puntos de Distribución de CRL» de cada certificado emitido. La ubicación base es: http://ca-subordinada-crl-darkcam-v2.s3.us-east-1.amazonaws.com/crl/
- **Servicio de Validación en Línea (OCSP):** La URL del respondedor OCSP se encuentra embebida en la extensión «Acceso a Información de la Autoridad» de cada certificado emitido. El endpoint es: http://ocsp.acm-pca.us-east-1.amazonaws.com

Detalle técnico de la arquitectura de los repositorios: (i) Repositorio del certificado de la SubCA y de esta DPC, publicado en el sitio web institucional (https://www.universe-id.com) sobre infraestructura HTTPS. (ii) Repositorio de CRL, alojado en buckets de Amazon S3 dedicados en la región us-east-1 con acceso público de solo lectura: «ca-subordinada-crl-darkcam-v2» para los certificados estándar y «ca-subordinada-short-crl-darkcam-v2» para los certificados de corta duración. Por tratarse de CRL particionadas (partitioned CRL) de AWS Private CA, la URL operativa de cada CRL es específica de su partición y se publica embebida en la extensión «Puntos de Distribución de CRL» de cada certificado; por diseño, no existe un nombre de archivo único y estático para la CRL. (iii) Repositorio OCSP, atendido por el respondedor gestionado de AWS Private CA, disponible de forma continua (24/7) en http://ocsp.acm-pca.us-east-1.amazonaws.com, cuya dirección se publica en la extensión «Acceso a Información de la Autoridad» de cada certificado.

2.2. Publicación de Información sobre Certificación

Toda la información relevante, incluyendo esta DPC, el certificado de la SubCA y las CRL, está disponible en los repositorios públicos. La CRL es firmada digitalmente por la SubCA DARKCAM para garantizar su autenticidad e integridad.

De forma específica, DARKCAM S.A. publica: (i) esta DPC y el certificado de la SubCA, en el sitio web institucional (https://www.universe-id.com); (ii) las Listas de Revocación de Certificados (CRL), en los buckets de Amazon S3 indicados en la sección 2.1, accesibles mediante la URL embebida en cada certificado; y (iii) las respuestas de estado en línea (OCSP), a través del respondedor gestionado de AWS Private CA. La información crítica de la PKI (claves privadas de las CA, registros de auditoría y configuraciones) NO es de acceso público: reside en componentes protegidos (HSM y buckets con acceso restringido) y su consulta o administración está limitada a roles autorizados mediante IAM con mínimo

privilegio y autenticación multifactor (MFA), conforme a la política de control de acceso descrita en la sección 2.4.

2.3. Frecuencia de la Publicación

Las CRL se publican de manera periódica de acuerdo con las políticas definidas por la SubCA DARKCAM. La frecuencia de actualización está embebida en el campo «Próxima Actualización» de cada CRL. El respondedor OCSP proporciona respuestas en tiempo real sobre el estado de los certificados.

Frecuencia exacta: **Frecuencia de actualización:** Las Listas de Certificados Revocados (CRL) serán actualizadas y publicadas **diariamente**, de conformidad con los requisitos aplicables a las Entidades de Certificación Acreditadas. Adicionalmente, ante la revocación o suspensión de un certificado, se realizará una **actualización extraordinaria de la CRL**, sin esperar al siguiente ciclo diario, garantizando que el estado de revocación sea reflejado oportunamente. La infraestructura utilizará, de manera complementaria, el protocolo **OCSP (Online Certificate Status Protocol)** para la consulta del estado de los certificados en línea. Las CRL emplean el modelo particionado (partitioned CRL) de AWS Private CA; en consecuencia, la URL del punto de distribución es específica de cada certificado y se encuentra embebida en su extensión «Puntos de Distribución de CRL», por lo que no corresponde a una dirección estática única.

2.4. Controles de Acceso a los Repositorios

Los repositorios son de acceso público y de solo lectura. DARKCAM S.A. implementa los controles de seguridad de AWS para proteger la integridad de la información publicada contra accesos no autorizados.

Mientras que la lectura de los repositorios es pública, toda operación de escritura o administración sobre la infraestructura que los soporta está sujeta a los siguientes controles: (i) Autenticación y autorización mediante AWS IAM con políticas de mínimo privilegio y control de acceso basado en roles (RBAC); (ii) Autenticación multifactor (MFA) obligatoria para toda acción administrativa; (iii) Garantía de integridad de los objetos publicados (CRL y certificados) mediante políticas de bucket de Amazon S3 y, donde aplica, S3 Object Lock, que impide su alteración o eliminación no autorizada; (iv) la CRL es firmada digitalmente por la SubCA DARKCAM, lo que permite a las partes de confianza verificar criptográficamente su autenticidad e integridad; y (v) registro y trazabilidad de todos los accesos y cambios mediante AWS CloudTrail. DARKCAM S.A. revisa periódicamente estos controles como parte de sus auditorías de cumplimiento.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Nombres

3.1.1. Tipos de Nombres y Perfiles de Certificado

Todos los certificados emitidos cumplen con el estándar X.509 v3. Los campos del Nombre Distinguido (DN) se asignan de acuerdo al tipo de certificado, basándose en la información verificada durante el proceso de registro automatizado.

La siguiente matriz detalla la estructura de los campos para cada perfil de certificado:

Atributo (DN)	P. Natural	P. Nat. RUC	Miembro Emp.	Rep. Legal	Sello Elec.
countryName (C)	EC	EC	EC	EC	EC
commonName (CN)	Nombres y Apellidos	Nombres y Apellidos	Nombres y Apellidos	Nombres y Apellidos	Razón Social
serialNumber	IDCEC-[cédula]	IDCEC-[cédula]	IDCEC-[cédula]	IDCEC-[cédula]	VATEC-[ruc]
surname	Apellidos	Apellidos	Apellidos	Apellidos	N/A
givenName	Nombres	Nombres	Nombres	Nombres	N/A
organization (O)	N/A	N/A	Razón Social	Razón Social	Razón Social
organizationalUnit (OU)	N/A	N/A	Depto. (Opc.)	N/A	N/A
title (T)	N/A	N/A	Cargo	REP. LEGAL	N/A
organizationIdentifier	N/A	TINEC-[ruc]	VATEC-[ruc]	VATEC-[ruc]	VATEC-[ruc]
emailAddress (E)	Email	Email	Email	Email	Email empresa

Mecanismo criptográfico e identificación por tipo de certificado. Todos los certificados se emiten conforme al estándar X.509 v3, con par de claves RSA de 4096 bits y algoritmo de firma SHA-256 con RSA. El tipo de certificado determina los atributos del Nombre Distinguido (DN) que se verifican y el OID de política asignado: (i) Persona Natural (con y sin RUC): se verifica la identidad de la persona mediante prueba de vida y cotejo biométrico contra el Registro Civil del Ecuador; el RUC, cuando aplica, se valida ante el SRI (OID 1.3.6.1.4.1.64482.2.1.1). (ii) Miembro de Empresa: además de la identidad de la persona, se verifica su relación de dependencia y la existencia de la empresa (OID 1.3.6.1.4.1.64482.2.2.1). (iii) Representante Legal: se verifica adicionalmente la calidad de representante legal vigente de la organización (OID 1.3.6.1.4.1.64482.2.3.1). (iv) Sello Electrónico: identifica a la persona jurídica mediante su razón social y RUC, no a una persona natural (OID 1.3.6.1.4.1.64482.2.2.2). En todos los casos, la autenticación del solicitante para gestionar el ciclo de vida del certificado se realiza mediante su cuenta autenticada en la plataforma Universe-ID.

3.2. Validación Inicial de Identidad

El proceso de validación es 100% digital y automatizado a través de la plataforma Universe-ID. El flujo completo consta de las siguientes etapas:

1. **Registro del Solicitante:** El usuario crea una cuenta en Universe-ID proporcionando sus datos básicos de contacto.
2. **Inicio de Solicitud y Captura de Datos:** El solicitante inicia una solicitud de certificado y completa el formulario con sus datos personales, datos de la empresa (según el tipo de certificado) y la documentación requerida.
3. **Prueba de Vida (Liveness Detection):** El solicitante realiza una prueba de vida en tiempo real mediante **AWS Amplify Face Liveness Detection**, utilizando la cámara de su dispositivo. Este paso confirma que el solicitante es una persona real y se encuentra físicamente presente durante el proceso.
4. **Validación Biométrica de Identidad:** Una vez superada la prueba de vida, la plataforma compara automáticamente los datos biométricos faciales capturados contra los registros oficiales del **Registro Civil del Ecuador**. Adicionalmente, se valida la correspondencia de la cédula de identidad, RUC y/o datos de representación legal mediante integración API con fuentes oficiales de confianza.
5. **Aceptación de Términos:** El solicitante debe aceptar explícitamente los Términos y Condiciones del servicio.
6. **Aprobación de la Solicitud:** Si todas las validaciones anteriores son exitosas, la plataforma aprueba automáticamente la solicitud.
7. **Generación del Certificado:** El suscriptor genera su certificado estableciendo una contraseña personal que protegerá su archivo PKCS#12 (.p12). Esta contraseña es definida exclusivamente por el suscriptor y **DARKCAM S.A. no la almacena en ningún momento**.

Solo tras completar exitosamente todas estas etapas se emite el certificado de firma electrónica.

3.3. Identificación y Autenticación para Emisión y Revocación

Tanto la emisión inicial como las solicitudes de revocación posteriores se gestionan a través del portal Universe-ID. El suscriptor debe autenticarse en su cuenta para realizar estas acciones, garantizando que solo el titular legítimo puede gestionar el ciclo de vida de su certificado.

4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DEL CERTIFICADO

4.1. Solicitud de Certificado

Las solicitudes se realizan exclusivamente a través de la plataforma en línea Universe-ID.

4.2. Procesamiento de Solicitudes

El procesamiento es automático. Una vez que el solicitante completa el flujo de validación de identidad, la solicitud es aprobada o rechazada por el sistema sin intervención manual. El tiempo total del proceso, desde la solicitud hasta la emisión, es típicamente de **pocos minutos**, dependiendo de la disponibilidad de los servicios de validación externos.

4.2.2. Aprobación o Rechazo de Solicitudes de Certificado

La aprobación o rechazo de una solicitud es resuelta automáticamente por la plataforma con base en criterios objetivos y verificables. Una solicitud se APRUEBA únicamente cuando se cumplen, de forma concurrente, todas las condiciones siguientes: (i) la prueba de vida (liveness) se supera satisfactoriamente; (ii) la comparación biométrica facial contra los registros oficiales del Registro Civil del Ecuador resulta positiva; (iii) la cédula de identidad y, cuando aplica, el RUC y/o los datos de representación legal corresponden y se encuentran vigentes según las fuentes oficiales consultadas por API; (iv) la información del formulario es consistente con los datos verificados; y (v) el solicitante acepta expresamente los Términos y Condiciones del servicio. La solicitud se RECHAZA cuando cualquiera de estas condiciones no se cumple —por ejemplo, fallo de la prueba de vida, ausencia de coincidencia biométrica, datos no correspondientes o no vigentes, o inconsistencias documentales—. Todo rechazo queda registrado y el solicitante puede reiniciar el proceso una vez subsanada la causa.

4.3. Emisión del Certificado

Tras la aprobación de la solicitud, el suscriptor procede a generar su certificado a través de la plataforma Universe-ID. Durante este paso, el suscriptor establece una **contraseña personal** que es enviada de forma segura al backend de la plataforma. El servidor solicita la emisión del certificado a la SubCA DARKCAM, y empaqueta la clave privada junto con el certificado en un archivo PKCS#12 (.p12) cifrado con la contraseña proporcionada por el suscriptor. Una vez generado el archivo .p12, **la contraseña no se almacena en ningún sistema de DARKCAM S.A.**.

El archivo .p12 cifrado se almacena en la plataforma para permitir al suscriptor utilizarlo en operaciones de firma directamente desde Universe-ID, así como descargarlo para su uso en herramientas de firma externas. Toda operación que involucre el uso de la clave privada contenida en el .p12 (firma de documentos a través de la plataforma o descarga del archivo) requiere que el suscriptor ingrese su contraseña personal en cada ocasión, garantizando que **solo el titular legítimo puede acceder y utilizar su clave privada**.

4.4. Aceptación del Certificado

La descarga del archivo .p12 y la finalización exitosa del proceso en la plataforma Universe-ID constituyen la aceptación del certificado por parte del suscriptor.

4.5. Uso del Par de Claves y del Certificado

El suscriptor es el único responsable de la custodia de su contraseña y del uso de su clave privada. El certificado puede utilizarse de dos maneras:

- **Firma a través de la plataforma Universe-ID:** El suscriptor inicia sesión en la plataforma y, al momento de firmar un documento, ingresa su contraseña del .p12 para autorizar la operación. La contraseña se utiliza únicamente para descifrar la clave privada durante el proceso de firma y no se almacena.
- **Uso en herramientas externas:** El suscriptor puede descargar su archivo .p12 (proporcionando su contraseña para autorizar la descarga) y utilizarlo en cualquier aplicación de firma electrónica compatible con el estándar PKCS#12. En este caso, la custodia y protección del archivo descargado es responsabilidad exclusiva del suscriptor.

El suscriptor debe notificar a DARKCAM S.A. inmediatamente si sospecha que su contraseña o su clave privada han sido comprometidas, para proceder con la revocación inmediata del certificado.

4.5.1. Parámetros Criptográficos, Generación y Custodia de la Clave Privada

Parámetros criptográficos. Los certificados de suscriptor se emiten con par de claves RSA de 4096 bits y algoritmo de firma SHA-256 con RSA (sha256WithRSAEncryption). Las claves de la Root CA y de la SubCA son RSA de 4096 bits. Los certificados de corta duración (one-shot) se firman con SHA-512 con RSA. Estos parámetros cumplen y superan los mínimos exigidos (RSA 2048 bits y SHA-256).

Generación de la clave privada. El par de claves del suscriptor se genera de forma programática en el entorno seguro del backend de la plataforma Universe-ID al momento de la emisión. Las claves de las Autoridades de Certificación se generan y residen dentro de los HSM administrados por AWS Private CA, con certificación FIPS 140-2 Nivel 3 o superior, y nunca abandonan el perímetro del módulo.

Almacenamiento y custodia. Durante la emisión, el suscriptor define una contraseña personal que se transmite de forma segura (TLS) y se utiliza exclusivamente para cifrar el archivo PKCS#12 (.p12) que contiene la clave privada y el certificado. Una vez generado el archivo, dicha contraseña no se persiste ni se registra en ningún sistema de DARKCAM S.A.; no existe campo de almacenamiento de la contraseña en las bases de datos de la plataforma. El archivo .p12 cifrado se conserva en el almacenamiento de la plataforma únicamente para habilitar las operaciones de firma y descarga del propio suscriptor. Dado que la contraseña constituye un factor de conocimiento exclusivo del titular y no es almacenada por DARKCAM S.A., la entidad no puede descifrar el archivo ni utilizar la clave privada sin la participación directa del suscriptor: toda operación que involucre la clave privada exige el ingreso de la contraseña en cada ocasión, garantizando que la clave permanece bajo control exclusivo del titular. Como modalidad de mayor

aseguramiento, la plataforma admite certificados sobre Dispositivo Seguro de Creación de Firma (DSCF), en los que la clave privada se genera y permanece en el dispositivo del suscriptor sin egresar de él.

4.6. Renovación del Certificado

DARKCAM S.A. no renueva certificados utilizando el mismo par de claves. Para obtener un nuevo certificado antes del vencimiento, el suscriptor debe solicitar una nueva emisión. El proceso es simplificado para usuarios existentes cuya identidad ya ha sido verificada.

4.7. Re-emisión del Certificado

La re-emisión con un nuevo par de claves se trata como una nueva solicitud de certificado.

4.8. Modificación del Certificado

Los certificados emitidos no pueden ser modificados. Si la información del suscriptor cambia (ej. cambio de nombre, cargo, etc.), el certificado actual debe ser revocado y se debe emitir uno nuevo.

4.9. Certificados de Corta Duración (Short-Lived / One-Shot)

Para escenarios de firma única, la plataforma Universe-ID permite la emisión de certificados de corta duración a través de la **SubCA DARKCAM Short**. Estos certificados se emiten una sola vez con el propósito exclusivo de firmar un documento específico, tienen una validez máxima de un (1) día (24 horas) y no son reutilizables.

Debido a su naturaleza efímera, los certificados short-lived no requieren mecanismos de revocación tradicional (CRL/OCSP), ya que expiran automáticamente en un plazo breve. Este modelo reduce significativamente la superficie de riesgo asociada a la exposición prolongada de claves criptográficas.

4.10. Revocación del Certificado

- **Circunstancias para la Revocación:** Un certificado debe ser revocado si la clave privada se ve comprometida, la información del certificado deja de ser válida, o el suscriptor lo solicita.
- **Procedimiento:** La revocación se solicita a través del portal de autogestión de Universe-ID.
- **Tiempo de Procesamiento:** La revocación es **inmediata** tras la confirmación de la solicitud. El cambio se refleja instantáneamente en el respondedor OCSP y en la siguiente CRL publicada.

5. CONTROLES DE INSTALACIONES, GESTIÓN Y OPERACIONES

5.1. Controles Físicos y del Entorno

DARKCAM S.A. no opera centros de datos propios. Toda su infraestructura tecnológica reside en plataformas de proveedores de nube líderes a nivel mundial.

- **Infraestructura PKI:** Se encuentra en los centros de datos de alta seguridad de **Amazon Web Services (AWS)**. AWS es responsable de la seguridad física, controles de acceso, redundancia de energía, climatización y protección contra desastres. Sus instalaciones cumplen con certificaciones internacionales como ISO/IEC 27001, SOC 1/2/3 y PCI DSS.
- **Microservicios y Base de Datos:** Se despliegan en infraestructuras gestionadas por **Google Cloud Platform** y **Supabase**, que aplican medidas de seguridad física y ambiental equivalentes.

5.2. Controles de Procedimiento

El acceso a los recursos en la nube está estrictamente controlado por roles y políticas de Mínimo Privilegio a través de los sistemas de Gestión de Identidad y Acceso (IAM) de los proveedores. Todas las acciones administrativas críticas requieren autenticación multifactor (MFA).

DARKCAM S.A. aplica el principio de segregación de funciones: las funciones críticas (emisión, revocación y administración de la PKI) están separadas mediante roles diferenciados en IAM, de modo que ninguna persona concentra el control total del ciclo de vida del certificado. Las operaciones más sensibles sobre la Autoridad de Certificación se sujetan a reglas de control multipersona (autorización por más de un rol) y quedan registradas de forma íntegra e inmutable en AWS CloudTrail para su posterior auditoría.

5.3. Controles de Personal

El personal de DARKCAM S.A. con acceso a la infraestructura cloud pasa por verificaciones de antecedentes y recibe capacitación continua en seguridad. Los roles están segregados para evitar conflictos de interés.

El personal con acceso a la infraestructura crítica suscribe acuerdos de confidencialidad como condición de su vinculación, recibe capacitación periódica sobre sus responsabilidades específicas y las políticas de seguridad de la información, y está sujeto a un procedimiento formal de desvinculación que contempla la revocación inmediata de todos sus accesos, credenciales y permisos sobre los sistemas de la PKI.

5.4. Registros de Auditoría

- **Fuente de Registros: AWS CloudTrail** registra todas las llamadas a la API realizadas en la infraestructura PKI, proporcionando una traza de auditoría completa e inmutable.
- **Eventos Registrados:** Se registran todos los eventos, incluyendo, pero no limitado a: IssueCertificate, RevokeCertificate, cambios en políticas de IAM, y accesos a la consola.

- **Periodo de Retención:** Conforme a la normativa ARCOTEL, los registros de auditoría se almacenan de forma segura en un bucket de AWS S3 por un período de **siete (7) años**, con políticas que garantizan su inmutabilidad (S3 Object Lock).

5.5. Continuidad del Negocio y Recuperación ante Desastres

La arquitectura nativa de la nube está diseñada para alta disponibilidad y resiliencia. Los servicios se despliegan en múltiples zonas de disponibilidad (Multi-AZ) para tolerar fallos de componentes individuales sin interrumpir el servicio. Se realizan copias de seguridad automáticas y periódicas de las bases de datos y configuraciones críticas.

5.6. Compromiso de Claves y Recuperación ante Desastres

Ante el compromiso, o la sospecha de compromiso, de la clave privada de una Autoridad de Certificación, DARKCAM S.A. activará su procedimiento de respuesta a incidentes, que contempla: la evaluación inmediata del alcance, la revocación de la CA afectada y de los certificados emitidos bajo ella, la notificación a la ARCOTEL y a los suscriptores y partes de confianza afectados, y la re-emisión de una nueva jerarquía o certificados según corresponda. En caso de compromiso de la clave de un suscriptor, este debe notificarlo de inmediato para proceder con la revocación, conforme a la sección 4.10.

Para la recuperación ante desastres, además de lo señalado en la sección 5.5, las claves de las CA se encuentran protegidas y respaldadas dentro de los HSM administrados por AWS Private CA, lo que permite restablecer la operación de la PKI ante la pérdida de componentes. Los objetivos de recuperación (RTO/RPO) se sustentan en la redundancia Multi-AZ, las copias de seguridad automáticas y la naturaleza administrada de los servicios utilizados, garantizando la continuidad de los servicios de validación (CRL y OCSP).

5.7. Terminación de las Actividades de la CA o de la RA

5.7.1. Notificación previa. En caso de cese, total o parcial, de las actividades de certificación, DARKCAM S.A. notificará dicha circunstancia a la ARCOTEL y a los suscriptores de sus certificados **con por lo menos noventa (90) días de anticipación**, conforme al artículo 35 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y al artículo 13 de su Reglamento General. La notificación a los suscriptores se realizará al correo electrónico registrado y mediante aviso destacado y permanente en https://www.universe-id.com.

5.7.2. Plan de cese ordenado. El cese se ejecutará conforme a un plan que contempla, como mínimo: (i) suspensión de la aceptación de nuevas solicitudes de emisión desde la fecha de la notificación; (ii) mantenimiento de los servicios de validación de estado (CRL y OCSP) y de revocación hasta la fecha efectiva de cese; (iii) revocación de la totalidad de los certificados que sigan vigentes a la fecha efectiva de cese, previa notificación individual a cada suscriptor; (iv) publicación de una CRL final; y (v) destrucción segura y documentada del material criptográfico de las Autoridades de Certificación dentro de los

módulos de seguridad de hardware, con acta suscrita por los responsables designados y notificación a la ARCOTEL.

5.7.3. Transferencia de certificados a otra entidad. DARKCAM S.A. podrá gestionar, en coordinación con la ARCOTEL, la transferencia de sus certificados vigentes a otra entidad de certificación acreditada que cumpla los mismos requisitos tecnológicos. **La cesión de certificados de firma electrónica de una entidad a otra requerirá la autorización expresa del titular del certificado**, conforme al artículo 13 del Reglamento General. Los suscriptores que no autoricen la cesión mantendrán su derecho a la revocación de su certificado conforme al numeral anterior.

5.7.4. Custodia de la información. Los expedientes de certificación, evidencias de validación de identidad, registros de auditoría y demás información sujeta a conservación serán transferidos a la entidad de certificación cesionaria o entregados a la ARCOTEL, según esta disponga, garantizando su integridad, confidencialidad y disponibilidad durante el plazo de retención señalado en las Secciones 5.4 y 9.4.8, y preservando la verificabilidad de las firmas electrónicas generadas con anterioridad al cese.

5.7.5. Garantía y obligaciones pendientes. La garantía de responsabilidad descrita en la Sección 9.2 se mantendrá vigente hasta la extinción de las obligaciones y responsabilidades derivadas de los certificados emitidos, conforme a lo que disponga la ARCOTEL. El cese de actividades no exime a DARKCAM S.A. de las responsabilidades adquiridas frente a suscriptores, partes de confianza y la autoridad de control con anterioridad a la fecha efectiva de terminación.

5.7.6. Terminación de la función de Autoridad de Registro. Dado que la función de Autoridad de Registro se ejecuta de forma automatizada por la propia plataforma Universe-ID (Sección 1.3.2), su terminación se produce simultáneamente con el cese de las actividades de la Autoridad de Certificación y se sujeta al mismo procedimiento.

6. CONTROLES TÉCNICOS DE SEGURIDAD

6.1. Generación e Instalación de Pares de Claves

- **Claves de la CA:** Las claves de la Root CA y la SubCA se generan y almacenan de forma segura dentro de los HSMs gestionados por AWS Private CA. Estas claves nunca abandonan el perímetro del HSM.
- **Claves del Suscriptor:** El par de claves del suscriptor se genera en el entorno seguro del backend de la plataforma durante el proceso de emisión. La contraseña definida por el suscriptor se transmite de forma segura al servidor, donde se utiliza exclusivamente para cifrar el archivo PKCS#12 (.p12) que contiene la clave privada y el certificado. Una vez generado el .p12, la contraseña no se persiste en ningún sistema. El archivo .p12 cifrado se almacena en la plataforma para permitir operaciones de firma y descarga, pero **DARKCAM S.A. no almacena ni**

tiene acceso a la contraseña del suscriptor. Toda operación que requiera el uso de la clave privada exige que el suscriptor ingrese su contraseña, asegurando que la clave privada permanece inaccesible sin el factor de conocimiento exclusivo del titular.

6.2. Protección de la Clave Privada y Módulos Criptográficos

- **Estándares Criptográficos:** Los HSMs que protegen las claves de la CA cumplen con la certificación **FIPS 140-2 Nivel 3 o superior**.
- **Tamaño de las Claves:**
  - **Root CA y SubCA:** RSA 4096 bits.
  - **Certificados de Suscriptor:** RSA 4096 bits, con algoritmo de firma SHA-256.

6.3. Controles de Seguridad Informática

La infraestructura está protegida por múltiples capas de seguridad, incluyendo políticas de red restrictivas, firewalls de aplicaciones web (WAF), protección contra DDoS y monitoreo de seguridad continuo a través de Datadog. Se realizan evaluaciones de vulnerabilidad y pruebas de penetración periódicas.

6.4. Datos de Activación

Los datos de activación de las claves de la Root CA y de la SubCA (PIN, fragmentos de activación y credenciales del módulo criptográfico) son generados y gestionados internamente por el HSM administrado de AWS Private CA, conforme a la certificación FIPS 140-2 Nivel 3 o superior, y nunca son expuestos ni manipulados por personal de DARKCAM S.A. Para los certificados de suscriptor, el dato de activación es la contraseña personal definida por el titular, que se utiliza para cifrar el archivo PKCS#12 (.p12); dicha contraseña constituye un factor de conocimiento exclusivo del suscriptor y no es almacenada por DARKCAM S.A.

6.5. Controles de Seguridad Informática

Adicionalmente a lo señalado en la sección 6.3, los sistemas que soportan la PKI aplican controles de seguridad informática heredados y propios: gestión de identidades y accesos mediante AWS IAM con mínimo privilegio y autenticación multifactor (MFA) obligatoria; sistemas operativos y servicios gestionados con parcheo continuo a cargo del proveedor de nube; cifrado en reposo (AWS KMS / SSE) y en tránsito (TLS) de la información sensible; y registro centralizado de eventos de seguridad. Los proveedores de infraestructura (AWS, Google Cloud) mantienen certificaciones ISO/IEC 27001, SOC 1/2/3 y PCI DSS que respaldan estos controles.

6.6. Controles Técnicos del Ciclo de Vida del Sistema

El software de la plataforma se desarrolla siguiendo prácticas de desarrollo seguro: control de versiones centralizado, revisión de código, gestión de cambios y despliegues controlados mediante canalizaciones

de integración y entrega continua (CI/CD). Los componentes se ejecutan sobre servicios administrados (Google Cloud Run para los microservicios de backend y Vercel para el frontend), lo que asegura entornos reproducibles, control de dependencias y la aplicación oportuna de actualizaciones de seguridad a lo largo de todo el ciclo de vida del sistema.

6.7. Controles de Seguridad de la Red

La PKI opera sobre servicios administrados de AWS que no requieren configuración de red tradicional: el acceso a la Autoridad de Certificación se realiza exclusivamente vía AWS SDK con autenticación IAM y credenciales temporales. La capa de aplicación está protegida por un firewall de aplicaciones web (WAF), protección contra denegación de servicio (DDoS), segmentación lógica de redes y comunicaciones cifradas con TLS. La Root CA permanece en estado offline, aislada de la red, y solo se activa para firmar el certificado de la SubCA. El tráfico y los eventos de red son monitoreados de forma continua mediante Datadog, y la totalidad de las llamadas a la API de la PKI queda registrada en AWS CloudTrail para su análisis y detección de anomalías.

7. PERFILES DE CERTIFICADO, CRL Y OCSP

7.1. Perfil del Certificado

Todos los certificados son X.509 v3 y cumplen con los perfiles definidos en los RFC correspondientes. La estructura detallada para cada tipo de certificado se especifica en la matriz de la sección 3.1.1. Las extensiones críticas como Key Usage (digitalSignature, nonRepudiation) y Basic Constraints se configuran adecuadamente.

Perfil técnico común de los certificados de entidad final (campos base, conforme a RFC 5280):

- Version: v3 (valor 2). Serial Number: entero positivo único asignado por la CA. Signature Algorithm: sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11).
- Issuer: C=EC, O=DARKCAM S.A., OU=CA Emisora de Certificados, ST=Pichincha, L=Quito, CN=DARKCAM S.A. - CA Subordinada. Validity: campos notBefore y notAfter (vigencia de hasta cinco (5) años para certificados de suscriptor). Subject: conforme a la matriz de la sección 3.1.1. Subject Public Key Info: RSA 4096 bits (rsaEncryption, OID 1.2.840.113549.1.1.1).
- Extensiones (X.509 v3): Key Usage (crítica): digitalSignature, nonRepudiation, keyEncipherment. Extended Key Usage: emailProtection (1.3.6.1.5.5.7.3.4) y clientAuth (1.3.6.1.5.5.7.3.2). Basic Constraints (crítica): cA=FALSE. Certificate Policies: OID de política según el tipo de certificado (rama 1.3.6.1.4.1.64482), con los calificadores CPS URI (https://universe-id.com/darkcam/cps.pdf) y User Notice. CRL Distribution Points: URL de la partición de CRL correspondiente al certificado. Authority Information Access: acceso OCSP (http://ocsp.acm-pca.us-east-1.amazonaws.com). Subject Key Identifier y Authority Key Identifier conforme a RFC 5280.

7.2. Perfil de la CRL

Las CRL son versión 2 y cumplen con el perfil RFC 5280. Contienen la fecha de emisión, fecha de próxima actualización y la lista de números de serie de los certificados revocados.

El perfil de la CRL comprende: campo Version v2; Issuer correspondiente a la SubCA DARKCAM emisora; los campos thisUpdate (fecha de emisión) y nextUpdate (próxima actualización, fijada en un máximo de 24 horas); la lista de certificados revocados con su número de serie y fecha de revocación (revocationDate); y las extensiones CRL Number y Authority Key Identifier. Por tratarse de CRL particionadas, cada CRL incluye además la extensión Issuing Distribution Point (IDP) que delimita su partición. La CRL es firmada por la SubCA emisora con el algoritmo sha256WithRSAEncryption, garantizando su autenticidad e integridad.

7.3. Perfil del OCSP

El respondedor OCSP cumple con el estándar RFC 6960, proporcionando un método de validación de estado de certificados en tiempo real.

Cada respuesta OCSP indica el estado del certificado consultado (good, revoked o unknown), incluye las marcas temporales thisUpdate y nextUpdate, y va firmada digitalmente para garantizar su autenticidad. El respondedor es el servicio gestionado por AWS Private CA, disponible de forma continua (24/7), y su URL se publica en la extensión Authority Information Access de cada certificado.

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

DARKCAM S.A. se somete a auditorías externas anuales por parte de una **entidad de inspección independiente acreditada por el Servicio de Acreditación Ecuatoriano (SAE)** y cualificada para verificar el cumplimiento de las prácticas descritas en esta DPC y la normativa de ARCOTEL. Los resultados de la auditoría se presentan a la autoridad regulatoria y se utilizan para implementar mejoras continuas en los procesos y controles.

Las auditorías de cumplimiento se realizan con periodicidad anual y están a cargo de una entidad de inspección independiente. DARKCAM S.A. se compromete a remitir a la ARCOTEL los informes de auditoría dentro de un plazo máximo de quince (15) días hábiles contados desde su emisión, acompañados de un Plan de Remediación que detalle, para cada hallazgo o no conformidad detectada, las acciones correctivas y los plazos definidos para su subsanación.

9. OTROS ASUNTOS COMERCIALES Y LEGALES

9.1 Tarifas

9.1.1. Tarifas

DARKCAM S.A. publica de forma transparente las tarifas aplicables a sus servicios de certificación, las cuales se encuentran disponibles en la plataforma web de DARKCAM.

PERSONA NATURAL / REPRESENTANTE LEGAL / MIEMBRO DE EMPRESA

Duración del certificado	Precio base (sin IVA)
1 año	**$14,78**
2 años	**$23,47**
3 años	**$31,30**
4 años	**$39,12**
5 años	**$46,08**

Certificado de firma de un solo uso (one-shot)
Valor desde $0.60 HASTA $5 dólares estadounidense

Certificados no comercializados a la fecha. Los certificados de **Sello Electrónico** y de **Sello de Tiempo**, así como la modalidad sobre Dispositivo Seguro de Creación de Firma (DSCF), se encuentran contemplados en esta DPC y cuentan con OID de política asignado, pero **su comercialización no se encuentra habilitada a la fecha de publicación de este documento**. Sus tarifas serán publicadas en el sitio web con anterioridad

a su puesta en servicio, conforme al procedimiento de la Sección 9.1.5, y esta DPC será actualizada conforme a la Sección 9.12.

9.1.2. Tarifas de otros servicios.

Renovación (nueva emisión): Mismos valores que el punto 9.1.1. Re-emisión por pérdida de contraseña o compromiso de clave: Mismos valores que el punto 9.1.1. **Revocación del certificado: sin costo. Consulta del estado de un certificado (CRL y OCSP): servicio público y gratuito para suscriptores y partes de confianza.** Acceso a esta DPC, a las Políticas de Certificación y al certificado de la SubCA: gratuito.

9.1.3. Condiciones de pago.

Los valores se facturan conforme a la normativa tributaria ecuatoriana y se cancelan de forma previa a la emisión, a través de los medios de pago habilitados en la plataforma (tarjeta de crédito/débito). Los precios incluyen los impuestos que legalmente correspondan cuando así se indique.

9.1.4. Política de reembolso. Conforme a la Sección 11 de los Términos y Condiciones, los valores pagados no son reembolsables una vez iniciado el proceso de validación, verificación, emisión, entrega o activación del servicio. Únicamente procede devolución total o proporcional cuando exista resolución expresa de DARKCAM S.A. que determine una falla exclusivamente imputable a la entidad que haga imposible la prestación del servicio contratado.

9.1.5. Modificación de tarifas. Toda modificación de tarifas se publica en el sitio web con anterioridad a su entrada en vigor y no afecta a los certificados ya emitidos durante su período de vigencia.

9.2. Responsabilidad Financiera

9.2.1. Garantía de responsabilidad. En cumplimiento del artículo 30, literal h) de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, y del artículo 13 de su Reglamento General, DARKCAM S.A. mantiene vigente una **póliza de seguro de responsabilidad civil** destinada a cubrir los daños y perjuicios que se ocasionen por el incumplimiento de las obligaciones previstas en la Ley y hasta por culpa leve en el desempeño de sus obligaciones.

9.2.2. Datos de la póliza vigente.

Concepto	Detalle
Aseguradora	SWEADEN COMPAÑÍA DE SEGUROS S.A.
Ramo	Responsabilidad Civil
N.° de póliza	0057970
Asegurado / Contratante	DARKCAM S.A. — RUC 1793185541001
Suma asegurada	USD 400.000,00 (cuatrocientos mil dólares de los Estados Unidos de América)
Vigencia	Desde las 12h00 del 13/03/2026 hasta las 12h00 del 13/03/2027
Beneficiario del endoso	Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL)

Concepto	Detalle
Condiciones generales	Aprobadas por la Superintendencia de Bancos y Seguros N.° 2008-042 de 30/01/2008
Deducible	10% del valor del siniestro, no menor a USD 5.000,00
Aviso de siniestro	5 días calendario

9.2.3. Naturaleza de la garantía. La póliza es **incondicional, irrevocable y de cobro inmediato**, y se emite a favor de la ARCOTEL, la que consta en sus condiciones particulares mediante endoso aclaratorio/modificatorio. Su monto satisface el mínimo exigido por el artículo 13 del Reglamento General a la Ley de Comercio Electrónico para el primer año de operación de una entidad de certificación acreditada.

9.2.4. Objeto y alcance de la cobertura. La garantía tiene por objeto precautelar y garantizar a los usuarios la adecuada prestación de los servicios de certificación de información y servicios relacionados, así como el cabal cumplimiento de las obligaciones previstas en la normativa vigente, en esta DPC y en el contrato de prestación de servicios suscrito con los usuarios. DARKCAM S.A. responde por los daños y perjuicios que se produzcan cuando: (i) actúe con negligencia; (ii) se derive del uso indebido del certificado de firma electrónica acreditado por causa imputable a la entidad; (iii) no haya consignado de forma clara en los certificados el límite de su uso y el tipo de transacciones válidas que pueden realizarse; o (iv) los datos consignados hayan sido afectados por culpa de la entidad, hasta por culpa leve.

9.2.5. Exención. DARKCAM S.A. queda exenta de responsabilidad por daños y perjuicios cuando el usuario exceda los límites de uso indicados en la política del certificado digital y en la póliza, o cuando la afectación no se produzca por culpa de la entidad.

9.2.6. Monto de indemnización. Para todos los eventos cubiertos, la indemnización por cada siniestro será de hasta el **100% del valor comercializado del certificado digital de firma electrónica emitido al usuario**, conforme al tipo de certificado (certificado de un solo uso, certificado en formato nube de larga duración y certificado en formato P12 de larga duración), según la tabla de tarifas de la Sección 9.1 vigente a la fecha de emisión del certificado.

9.2.7. Trámite de reclamos. Todo reclamo presentado por un usuario de la entidad de certificación será tramitado y resuelto conforme al artículo innumerado 14 del Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, que prevé un término de quince (15) días para la presentación del reclamo motivado ante la autoridad de control, cinco (5) días para la respuesta de la entidad y cinco (5) días para la resolución de la autoridad.

9.2.8. Renovación y vigencia continua. DARKCAM S.A. se obliga a mantener la garantía vigente e ininterrumpida durante todo el período de su acreditación, a renovarla con anterioridad a su vencimiento y a remitir a la ARCOTEL el original y copia de la póliza renovada, así como a informar cualquier modificación de sus condiciones o monto asegurado.

9.3. Confidencialidad de la Información del Negocio

DARKCAM S.A. trata como confidencial toda la información que no está destinada a publicación, incluyendo los datos personales de los suscriptores, los registros internos de operación y, en particular, las claves privadas y los datos de activación. No se considera confidencial, por su naturaleza pública, la información contenida en los certificados emitidos, las CRL, las respuestas OCSP y la presente DPC. El acceso a la información confidencial se restringe conforme a las políticas de control de acceso descritas en las Secciones 2.4 y 5.

9.4. Privacidad de los Datos Personales

9.4.1. Marco aplicable y rol. DARKCAM S.A. actúa como **responsable del tratamiento** de los datos personales de solicitantes y suscriptores, conforme a la Ley Orgánica de Protección de Datos Personales (LOPDP) y su Reglamento General. El detalle completo del tratamiento consta en la Política de Protección de Datos Personales publicada en https://www.universe-id.com/politica-privacidad

9.4.2. Datos tratados y finalidades. Se tratan datos de identificación (nombres, cédula, RUC), de contacto (correo electrónico, teléfono), datos de representación o vínculo laboral y **datos biométricos faciales** obtenidos durante la prueba de vida y el cotejo contra el Registro Civil del Ecuador. Las finalidades son las descritas en la Sección 6 de los Términos y Condiciones: verificación de identidad y prevención de fraude y suplantación; gestión del ciclo de vida del certificado; cumplimiento de obligaciones legales, regulatorias, de auditoría y trazabilidad; mantenimiento de registros y evidencias; comunicaciones operativas y de seguridad; atención de solicitudes y reclamos; y gestión contractual y de facturación. Los datos biométricos se tratan con **consentimiento expreso e informado** del titular y de forma limitada a las finalidades de identificación, autenticación, prevención de fraude y cumplimiento regulatorio.

9.4.3. Base de licitud. El tratamiento se sustenta en (i) el consentimiento expreso, libre, específico e informado del titular; (ii) el cumplimiento de una obligación legal y regulatoria aplicable a las entidades de certificación acreditadas; y (iii) la ejecución de la relación contractual.

9.4.4. Encargados y transferencias. DARKCAM S.A. comunica datos a encargados del tratamiento necesarios para la prestación del servicio (proveedores de infraestructura en la nube, servicios de verificación biométrica y de prueba de vida, base de datos, monitoreo y auditoría), bajo contrato que impone obligaciones de confidencialidad y medidas de seguridad equivalentes. Algunos de estos proveedores procesan información fuera del territorio nacional, amparados en cláusulas contractuales y estándares de seguridad reconocidos internacionalmente. También se comunican datos a la autoridad competente cuando exista mandato legal, regulatorio, judicial o administrativo.

9.4.5. Medidas de seguridad. Cifrado en tránsito (TLS) y en reposo (AWS KMS/SSE); control de acceso basado en roles con mínimo privilegio y autenticación multifactor obligatoria; segregación de funciones; registro y trazabilidad íntegra e inmutable de accesos y operaciones (AWS CloudTrail y S3 Object Lock); monitoreo continuo; y evaluaciones periódicas de vulnerabilidades, conforme a las Secciones 2.4, 5 y 6 de esta DPC.

9.4.6. Ejercicio de los derechos del titular (ARCO y demás derechos LOPDP). El titular puede ejercer sus derechos de **acceso, rectificación y actualización, eliminación, oposición, portabilidad, suspensión del tratamiento y a no ser objeto de decisiones automatizadas**, mediante solicitud dirigida a administrativo@dark-cam.com o desde su cuenta autenticada en la plataforma Universe-ID, adjuntando copia de su documento de identidad y precisando el derecho que ejerce. **DARKCAM S.A. atenderá la solicitud dentro del plazo de quince (15) días** contados desde su recepción, conforme a los artículos 13, 14, 15 y 16 de la LOPDP. El ejercicio de estos derechos es gratuito. Si la solicitud fuere denegada o no atendida, el titular puede presentar reclamo ante la Autoridad de Protección de Datos Personales.

9.4.7. Limitación al derecho de eliminación. El titular reconoce que la información contenida en un certificado emitido, en las CRL y en los registros de auditoría **no puede ser eliminada** mientras subsistan las obligaciones legales de conservación y la necesidad de garantizar el valor probatorio y la verificabilidad de las firmas electrónicas generadas, conforme al artículo 15 de la LOPDP.

9.4.8. Plazo de retención. Los expedientes de certificación, evidencias de validación de identidad, constancias de aceptación y registros de auditoría se conservan por un período de siete (7) años contados desde la expiración o revocación del certificado, en coherencia con el plazo de retención de registros de auditoría de la Sección 5.4 y con los plazos legales de conservación aplicables. Cumplido el plazo, la información se elimina o anonimiza de forma segura, salvo obligación legal o requerimiento de autoridad en contrario.

9.4.9. Delegado de Protección de Datos Personales. DARKCAM S.A. ha designado un Delegado de Protección de Datos Personales, conforme al artículo 48 de la LOPDP, dado el tratamiento a gran escala de categorías especiales de datos (datos biométricos). Contacto: administrativo@dark-cam.com

9.5. Derechos de Propiedad Intelectual

DARKCAM S.A. conserva los derechos de propiedad intelectual sobre esta DPC, las políticas de certificación, el software de la plataforma Universe-ID, sus marcas y los identificadores de objeto (OID) asignados a la entidad. El suscriptor conserva la titularidad sobre su propio par de claves.

9.6. Declaraciones y Garantías

9.6.1. Declaraciones y Garantías de la Autoridad de Certificación

DARKCAM S.A. garantiza que emite los certificados conforme a esta DPC, que verifica la identidad de los suscriptores según la Sección 3, y que mantiene operativos los servicios de revocación y validación de estado (CRL y OCSP).

9.6.2. Declaraciones y Garantías de la Autoridad de Registro

Las funciones de Autoridad de Registro se ejecutan de forma automatizada por la plataforma Universe-ID, conforme a lo descrito en la Sección 1.3.2, garantizando la verificación de identidad establecida en esta DPC.

9.6.3. Declaraciones y Garantías del Suscriptor

El suscriptor declara y garantiza que: (i) la información proporcionada para la emisión del certificado es veraz, completa y actualizada, y se compromete a mantenerla así; (ii) genera y custodia su clave privada y la contraseña de su archivo PKCS#12 (.p12) de forma personal, confidencial e intransferible, bajo su exclusivo control; (iii) notificará de inmediato a DARKCAM S.A. ante la pérdida, el robo o el compromiso de su clave privada o de sus credenciales, a fin de proceder con la revocación; (iv) utilizará el certificado únicamente para los fines autorizados en la Sección 1.4 y conforme a la legislación vigente; y (v) acepta y cumple los Términos y Condiciones del servicio.

9.6.4. Declaraciones de las Partes de Confianza

Las partes de confianza, antes de confiar en una firma electrónica, deben verificar el estado de revocación del certificado mediante la CRL o el servicio OCSP, validar la cadena de confianza hasta la Root CA y comprobar que el uso del certificado corresponde a los fines autorizados.

9.7. Renuncias de Garantías

Dentro de los límites permitidos por la legislación ecuatoriana, y sin perjuicio de las obligaciones legales y regulatorias que asume como entidad de certificación acreditada, DARKCAM S.A. declara que:

a) El certificado digital acredita el vínculo entre una clave pública y la identidad verificada de su titular conforme a la Sección 3 de esta DPC. **No constituye, por sí mismo, garantía del contenido, licitud, veracidad sustancial, exactitud, conveniencia económica, legalidad material, capacidad patrimonial, solvencia, intencionalidad, oportunidad ni ejecutabilidad** de los documentos, mensajes de datos, contratos o transacciones firmados con él.

b) DARKCAM S.A. **no garantiza la disponibilidad ininterrumpida ni la ausencia absoluta de errores** de sus plataformas, portales, validadores, repositorios, servicios OCSP, CRL, canales de atención ni de las infraestructuras de terceros de las que depende. Podrá suspender o limitar temporalmente los servicios por mantenimiento, actualización, contingencia, mitigación de incidentes, cumplimiento regulatorio o seguridad informática, sin que ello constituya incumplimiento.

c) DARKCAM S.A. **no responde por hechos atribuibles al suscriptor o a terceros**, incluyendo fallos de conectividad, energía, hardware o software del usuario, programas maliciosos, accesos indebidos originados en el entorno del usuario, suplantación derivada de información falsa proporcionada por el solicitante, negligencia del titular en la custodia de su clave privada o contraseña, e incumplimiento de las medidas de seguridad comunicadas.

d) DARKCAM S.A. **no responde por caso fortuito ni fuerza mayor**, conforme a la Sección 9.16.

e) Las presentes renuncias **no excluyen ni limitan** la responsabilidad de DARKCAM S.A. derivada de dolo, culpa grave o culpa leve en el desempeño de sus obligaciones legales, ni las coberturas de la garantía de responsabilidad descrita en la Sección 9.2, ni cualquier responsabilidad que por norma imperativa no sea renunciable.

9.8. Limitaciones de Responsabilidad

9.8.1. Alcance. La responsabilidad de DARKCAM S.A. se limita al cumplimiento diligente de los procedimientos de validación de identidad, emisión, administración, suspensión, revocación, publicación de estado y entrega del certificado, descritos en esta DPC, en las Políticas de Certificación y en los Términos y Condiciones del servicio, que constituyen el **Acuerdo de Suscriptor** aceptado por el titular con carácter previo a la emisión y disponible en https://www.universe-id.com.

9.8.2. Límite máximo de indemnización. En la máxima medida permitida por la ley, la responsabilidad acumulada total de DARKCAM S.A. frente al solicitante, al suscriptor o a terceros confiantes, por cualquier concepto vinculado a un certificado específico, **no excederá del valor efectivamente pagado por dicho certificado** o por el servicio directamente relacionado, en concordancia con la Sección 16 de los Términos y Condiciones y con el numeral 9.2.6 de esta DPC.

Tipo de certificado	Vigencia	Límite máximo de indemnización (USD)
Persona Natural / Rep. Legal / Miembro de Empresa	1 año	14,78
Persona Natural / Rep. Legal / Miembro de Empresa	2 años	23,47
Persona Natural / Rep. Legal / Miembro de Empresa	3 años	31,30
Persona Natural / Rep. Legal / Miembro de Empresa	4 años	39,12
Persona Natural / Rep. Legal / Miembro de Empresa	5 años	46,08
Certificado de un solo uso (one-shot)	24 horas	Valor unitario efectivamente pagado conforme al contrato corporativo

En todos los casos, la indemnización se sujeta al deducible y a la suma asegurada de la póliza descrita en la Sección 9.2 y corresponde al valor vigente a la fecha de emisión del certificado.

9.8.3. Cobertura agregada. Sin perjuicio del límite individual anterior, la cobertura agregada de los siniestros se sujeta a la suma asegurada de la póliza de responsabilidad civil descrita en la Sección 9.2 (USD 400.000,00) y a su deducible del 10% del valor del siniestro, no menor a USD 5.000,00.

9.8.4. Daños excluidos. En ningún caso DARKCAM S.A. responderá por daños indirectos, incidentales, especiales, punitivos, mediatos o consecuenciales, incluyendo lucro cesante, pérdida de oportunidades de negocio, pérdida de ingresos, pérdida de reputación, pérdida de datos, paralización de actividades, pérdida de contratos o afectaciones derivadas del contenido de los documentos firmados.

9.8.5. Exclusiones específicas. DARKCAM S.A. no responde cuando: (i) el usuario exceda los límites de uso establecidos en la Sección 1.4 y en la política del certificado; (ii) la parte de confianza omita verificar el estado de revocación del certificado por CRL u OCSP y la validez de la cadena de confianza, conforme a la Sección 9.6.4; (iii) el daño se produzca antes de la recepción y procesamiento de una solicitud válida de

suspensión o revocación; o (iv) el daño derive de información falsa o inexacta proporcionada por el solicitante.

9.8.6. Norma imperativa. Los límites anteriores no aplican cuando una norma imperativa de la legislación ecuatoriana disponga un límite distinto no renunciable.

9.9. Indemnizaciones

9.9.1. Indemnización por parte del suscriptor. El solicitante, el suscriptor y, en su caso, la persona jurídica a cuyo nombre se emite el certificado, se obligan a defender, mantener indemne y sacar en paz y a salvo a DARKCAM S.A., sus accionistas, administradores, funcionarios, dependientes, terceros vinculados, proveedores y contratistas, frente a toda reclamación, acción, procedimiento, sanción, multa, daño, costo, gasto u honorario profesional derivado de:

a) información falsa, inexacta, incompleta o desactualizada proporcionada durante la solicitud o durante la vigencia del certificado;
b) uso indebido, negligente, fraudulento o no autorizado del certificado;
c) incumplimiento de esta DPC, de las Políticas de Certificación, de los Términos y Condiciones o de la normativa aplicable;
d) pérdida, divulgación, compromiso o mal manejo de la clave privada o de la contraseña que protege el archivo PKCS#12;
e) omisión de solicitar oportunamente la suspensión o revocación del certificado ante un evento que afecte su confiabilidad;
f) reclamaciones de terceros fundadas en actos o declaraciones suscritas con el certificado del titular;
g) controversias sobre representación, mandato, facultades o legitimación del solicitante.

9.9.2. Indemnización por parte de las partes de confianza. La parte de confianza que sufra un daño por haber confiado en un certificado sin verificar previamente su estado de vigencia y revocación, la validez de la cadena de confianza y la pertinencia del tipo de certificado para la transacción concreta, asume dicho daño de forma exclusiva y mantendrá indemne a DARKCAM S.A. frente a reclamaciones de terceros derivadas de esa omisión.

9.9.3. Supervivencia. Las obligaciones de indemnidad previstas en esta sección subsisten aun después de la terminación de la relación contractual, de la expiración o de la revocación del certificado.

9.10. Vigencia y Terminación

9.10.1. Vigencia. Esta DPC entra en vigor en la fecha indicada en su cabecera y permanece vigente hasta su reemplazo por una versión posterior publicada en el repositorio público.

9.10.2. Terminación. La vigencia de esta DPC termina por su sustitución por una versión posterior, por el cese de actividades de DARKCAM S.A. conforme a la Sección 5.7, o por resolución de la autoridad competente que deje sin efecto la acreditación.

9.10.3. Supervivencia. No obstante la terminación, subsisten las obligaciones de confidencialidad (9.3), protección de datos personales y conservación de registros (9.4), indemnidad (9.9), limitaciones de

responsabilidad (9.8) y resolución de disputas (9.13), respecto de todos los certificados emitidos durante su vigencia.

9.11. Notificaciones y Comunicaciones

Las notificaciones y comunicaciones entre DARKCAM S.A. y los suscriptores se realizan a través de la plataforma Universe-ID y del correo electrónico registrado por el suscriptor.

9.12. Modificaciones (Enmiendas)

9.12.1. Procedimiento. Las modificaciones a esta DPC son propuestas, revisadas y aprobadas por el órgano señalado en la Sección 1.5.1. Toda nueva versión se identifica con un número de versión y una fecha de entrada en vigor, se incorpora al historial de cambios de la Sección 1.2 y se publica en https://universe-id.com/darkcam/cps.pdf.

9.12.2. Notificación. Las modificaciones sustanciales se comunican a los suscriptores al correo electrónico registrado y mediante aviso en la plataforma, con una anticipación mínima de (15) días a su entrada en vigor. Las modificaciones que obedezcan a cambios regulatorios, exigencias de seguridad, prevención de fraude o requerimiento de autoridad competente podrán entrar en vigor de forma inmediata desde su publicación.

9.12.3. Comunicación a la autoridad. Las modificaciones sustanciales se ponen en conocimiento de la ARCOTEL conforme a la normativa aplicable a las entidades de certificación acreditadas.

9.12.4. Cambio de OID. Las modificaciones que alteren de forma material los requisitos de validación de identidad o el nivel de confianza de un tipo de certificado darán lugar a la asignación de un nuevo Identificador de Objeto (OID) de política. Las modificaciones de forma, corrección de erratas o precisiones editoriales no implican cambio de OID.

9.13. Resolución de Disputas

9.13.1. Solución directa. Las partes procurarán resolver de forma directa y de común acuerdo toda controversia derivada de la prestación de los servicios de certificación. Los reclamos podrán presentarse a través de los canales indicados en la Sección 1.5.2 y serán atendidos en el plazo allí establecido.

9.13.2. Reclamos ante la autoridad de control. Sin perjuicio de lo anterior, el usuario podrá presentar su reclamo ante la ARCOTEL, el que se tramitará y resolverá conforme al artículo innumerado 14 del Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

9.13.3. Arbitraje. De no existir acuerdo directo, toda controversia, discrepancia, reclamación o litigio derivado de la existencia, validez, interpretación, ejecución, incumplimiento, terminación o efectos de la relación de servicio será resuelto en forma definitiva mediante **arbitraje administrado por el Centro de Arbitraje y Mediación de la Cámara de Comercio de Quito**, conforme a su reglamento vigente. El arbitraje será en derecho, la sede será la ciudad de Quito, Ecuador, y el idioma el español, conforme a la Sección 30 de los Términos y Condiciones. Lo anterior no impide a DARKCAM S.A. solicitar medidas cautelares o de tutela preventiva ante árbitros de emergencia o autoridad competente.

9.13.4. Ejecución de la garantía. Las controversias relativas a la ejecución de la garantía de responsabilidad descrita en la Sección 9.2 se sujetan al procedimiento previsto en la propia póliza y en la normativa de seguros aplicable.

9.14. Legislación Aplicable

Esta DPC y todos los servicios prestados por DARKCAM S.A. se rigen por las leyes y regulaciones de la **República del Ecuador**.

9.15. Cumplimiento de la Legislación Aplicable

DARKCAM S.A. presta sus servicios en cumplimiento de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su Reglamento General; de las resoluciones, regulaciones y normas técnicas emitidas por la ARCOTEL; de la Ley Orgánica de Protección de Datos Personales y su Reglamento; de la normativa tributaria y societaria ecuatoriana; y de las demás disposiciones que resulten aplicables. En caso de contradicción entre documentos, rige el orden de prelación establecido en la Sección 1 de los Términos y Condiciones: (a) la normativa imperativa vigente; (b) el acto administrativo de acreditación y la normativa técnica de la autoridad competente; (c) esta DPC y las Políticas de Seguridad; (d) las Políticas de Certificación; (e) los Términos y Condiciones; y (f) la solicitud o formulario específico.

9.16. Cláusulas Varias

9.16.1. Acuerdo íntegro. Esta DPC, las Políticas de Certificación, las Políticas de Seguridad, la Política de Protección de Datos Personales y los Términos y Condiciones constituyen el acuerdo íntegro entre DARKCAM S.A. y sus suscriptores respecto de los servicios de certificación.

9.16.2. Cesión. El suscriptor no podrá ceder, transferir, delegar ni gravar los derechos u obligaciones derivados del servicio sin autorización previa y escrita de DARKCAM S.A. DARKCAM S.A. podrá ceder, transferir, delegar, subcontratar o transmitir total o parcialmente sus derechos u obligaciones a compañías vinculadas, afiliadas, sucesoras o adquirentes, siempre que se preserve la continuidad del servicio y el cumplimiento regulatorio, y sin perjuicio de lo previsto en la Sección 5.7 para la cesión de certificados.

9.16.3. Nulidad parcial. Si una o varias disposiciones de esta DPC fueren declaradas nulas, inválidas o inejecutables, las restantes conservarán plena validez. La disposición afectada se interpretará o sustituirá de la manera que más se aproxime a su finalidad original dentro de los límites legales.

9.16.4. No renuncia. La falta de ejercicio o el ejercicio tardío por parte de DARKCAM S.A. de cualquiera de sus derechos no constituye renuncia ni impide su ejercicio posterior.

9.16.5. Fuerza mayor y caso fortuito. DARKCAM S.A. no será responsable por demoras, suspensión, interrupción o imposibilidad de prestar los servicios cuando ello obedezca a caso fortuito, fuerza mayor, hechos de terceros, fallas de proveedores esenciales, ciberataques generalizados, indisponibilidad de

infraestructura crítica, actos de autoridad, desastres naturales, interrupciones eléctricas o fallas de telecomunicaciones fuera de su control razonable.