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: Octubre 2025

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

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.

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 SHA512.
  - **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 SHA512.
  - **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.

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. **Validación Automatizada de Identidad:** Se integra vía API con fuentes oficiales de confianza (ej. Registro Civil del Ecuador) para verificar la autenticidad y correspondencia de los documentos de identidad y RUC.
3. **Verificación Biométrica:** Implementa una prueba de vida en tiempo real (Face Liveness Detection) para confirmar que el solicitante es una persona real y es el titular legítimo del documento de identidad presentado.

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).
  - **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.

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).

1.5. Administración de Políticas

- **Organización:** DARKCAM S.A.
- **Contacto:** Representante Legal
- **Correo Electrónico:** info@dark-cam.com
- **Página Web:** https://dark-cam.com

1.6. Definiciones y Acrónimos

- **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 dark-cam
- **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.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

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.

2.3. 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.

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 del Certificado (DN)	Persona Natural	P. Natural con RUC	Miembro de Empresa	Rep. Legal	Sello Electrónico
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-[cedula]	IDCEC-[cedula]	IDCEC-[cedula]	IDCEC-[cedula]	VATEC-[ruc]
surname	Apellidos	Apellidos	Apellidos	Apellidos	N/A
givenName	Nombres	Nombres	Nombres	Nombres	N/A
organization (O)	N/A	N/A	Razón Social Empresa	Razón Social Empresa	Razón Social
organizationalUnit (OU)	N/A	N/A	Departamento (Opc.)	N/A	N/A
title (T)	N/A	N/A	Cargo en la empresa	REPRESENTANTE LEGAL	N/A
organizationIdentifier	N/A	TINEC-[ruc]	VATEC-[ruc_empresa]	VATEC-[ruc]	VATEC-[ruc]
emailAddress (E)	Email del titular	Email del titular	Email del titular	Email del titular	Email de la empresa

3.2. Validación Inicial de Identidad

El proceso de validación es 100% digital y automatizado a través de la plataforma Universe-ID:

1. **Registro del Solicitante:** El usuario crea una cuenta en Universe-ID y completa el formulario de solicitud con sus datos personales o de la empresa.

2. **Verificación de Datos:** La plataforma se conecta mediante APIs a fuentes oficiales (ej. Registro Civil) para validar en tiempo real la correspondencia de la cédula de identidad, RUC y/o datos de representación legal.
3. **Verificación Biométrica de Identidad:** El solicitante debe completar exitosamente una prueba de vida (Face Liveness Detection) a través de la cámara de su dispositivo. Este paso asegura que la persona que realiza la solicitud es quien dice ser y está físicamente presente.
4. **Aceptación de Términos:** El solicitante debe aceptar explícitamente los Términos y Condiciones del servicio.

Solo tras completar exitosamente estos pasos, la plataforma aprueba la solicitud para la emisión del certificado.

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.

4.3. Emisión del Certificado

Tras la aprobación, la SubCA DARKCAM emite el certificado y la plataforma genera el archivo PKCS#12 (.p12) que contiene la clave privada y el certificado del suscriptor, protegido por una contraseña segura establecida por el propio usuario durante el proceso.

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 y el uso de su clave privada. Debe proteger la contraseña de su archivo .p12 y notificar a DARKCAM S.A. inmediatamente si sospecha que su clave ha sido comprometida.

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.

DARKCAM

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. 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).

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.

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.

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 durante el proceso de emisión. La clave privada se empaqueta de forma segura en un archivo .p12 cifrado con una contraseña que solo el suscriptor conoce. **DARKCAM S.A. no almacena ni tiene acceso a las claves privadas de sus suscriptores.**

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 2048 bits**.

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.

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.

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.

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.

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES
DARKCAM S.A. se somete a auditorías externas anuales por parte de una firma independiente 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.

9. OTROS ASUNTOS COMERCIALES Y LEGALES

9.1. Resolución de Disputas
Cualquier disputa se resolverá de acuerdo con los procedimientos establecidos en los Términos y Condiciones del servicio aceptados por el suscriptor.

9.2. 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**.