Certificamos Información Digital

POLÍTICA DE CERTIFICADOS PARA PERSONA NATURAL (PC-PN)	
SGSI - GG	Código: **PCPN-DES-DC-00019**
	Versión: 1.0
	Clasificación de Información: Documento de Acceso Público

POLÍTICA DE CERTIFICADOS PARA PERSONA NATURAL (PC-PN)

Aprobado por:	**Firma de Aprobación:**
Galo Santiago Becerra Gordón Gerente General	 Digitally signed by GALO SANTIAGO BECERRA GORDÓN
	Fecha de Aprobación: 05 de febrero de 2026

Tabla de Contenidos / Índice

POLÍTICA DE CERTIFICADOS PARA PERSONA NATURAL (PC-PN)

1. INTRODUCCIÓN

1.1 Visión General

Esta Política de Certificados (en adelante, **PC-PN**) establece las reglas, procesos, niveles de seguridad y responsabilidades legales que rigen el ciclo de vida de los certificados de firma electrónica emitidos exclusivamente a **Personas Naturales** por parte de DICERT.

La presente PC-PN se deriva y complementa a la Declaración de Prácticas de Certificación (**DPC**) de DICERT, la cual actúa como el marco operativo general. Los certificados emitidos bajo esta política garantizan la vinculación técnica y jurídica entre una clave pública y la identidad de una persona física, proporcionando los atributos de **autenticidad, integridad y no repudio** con plena validez legal en el territorio ecuatoriano, conforme a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

1.2 Nombre e Identificación del Documento

- **Nombre:** Política de Certificados para Persona Natural de DICERT.
- **Identificador de Objeto (OID):** 1.3.6.1.4.1.62486.2.1.1
- **Versión:** 1.0
- **Estado:** Vigente
- **Fecha de Publicación:** 5 de febrero de 2026
- **Ubicación:** https://www.dicert.com.ec/repositorio/pc-persona-natural

El OID especificado anteriormente deberá ser incluido obligatoriamente en la extensión *certificatePolicies* de todos los certificados emitidos bajo este perfil.

1.3 Participantes de la PKI

1.3.1 Autoridad de Certificación (AC): DICERT, en su calidad de Entidad de Certificación de Información acreditada por ARCOTEL, es la entidad responsable de la emisión, administración y revocación de estos certificados.

1.3.2 Autoridad de Registro (AR): Son las unidades encargadas de la validación presencial o remota (biométrica) de la identidad de los solicitantes, actuando bajo la delegación y control técnico de DICERT.

1.3.3 Suscriptores: Personas naturales, nacionales o extranjeras, que poseen capacidad legal para obligarse y que han superado con éxito el proceso de verificación de identidad de DICERT.

1.3.4 Partes Confiantes: Personas naturales o jurídicas que, basándose en la confianza de la jerarquía de DICERT, validan la firma electrónica del suscriptor mediante el uso de CRL o servicios OCSP.

1.4 Uso de los Certificados

1.4.1 Usos Permitidos: Los certificados emitidos bajo esta PC-PN están destinados para:

- Firma de documentos electrónicos personales.
- Trámites en portales gubernamentales (SRI, Aduana, IESS, etc.).
- Acceso a sistemas de banca en línea.
- Cifrado de mensajes de datos personales.

1.4.2 Usos Prohibidos: Se prohíbe expresamente el uso de estos certificados para:

- Actuar en representación legal de una persona jurídica (salvo que posea el certificado específico de representante).
- Emisión de certificados o sellado de tiempo (funciones propias de una AC).
- Actividades ilícitas que contravengan la seguridad nacional o los derechos de terceros.

1.5 Administración de la Política

1.5.1 Organización que administra el documento: DICERT S.A.S., a través de su Departamento Jurídico y Técnico.

1.5.2 Persona de contacto: Gerente General de DICERT. Correo: soporte@dicert.com.ec

1.5.3 Persona que determina la idoneidad de la PC para la política: La Gerencia General de DICERT, previa auditoría técnica de cumplimiento.

1.5.4 Procedimientos de aprobación: Toda modificación a esta PC-PN requiere la aprobación escrita de la Gerencia y la notificación inmediata a ARCOTEL para su registro en el expediente de la entidad.

1.6 Definiciones y Acrónimos

Para la interpretación de esta política, se aplicarán las definiciones contenidas en la **RFC 3647** y en la **DPC de DICERT**. En caso de discrepancia terminológica, prevalecerá lo establecido en la Ley de Comercio Electrónico de la República del Ecuador.

2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO

2.1 Repositorios

DICERT gestiona repositorios de información con alta disponibilidad (99.9%) operados sobre infraestructura de **AWS**, garantizando el acceso permanente a los usuarios y terceras partes confiantes. Estos repositorios son el medio oficial para la difusión de la normativa y el estado de los certificados emitidos bajo esta PC-PN.

2.2 Publicación de Información de Certificación

DICERT publica en su sitio web de forma abierta y gratuita:

1. La Declaración de Prácticas de Certificación (DPC) vigente.
2. La presente Política de Certificados para Persona Natural (PC-PN).
3. Los Certificados de la AC Raíz e Intermedia que conforman la cadena de confianza.
4. La Lista de Certificados Revocados (CRL).
5. El acceso al servicio de consulta en línea OCSP.

2.3 Tiempo o Frecuencia de Publicación

- **Políticas (DPC/PC):** Se publican inmediatamente tras su aprobación por la Gerencia y notificación a ARCOTEL.
- **CRL:** DICERT emite y publica una nueva CRL cada **veinticuatro (24) horas**. En caso de revocaciones críticas, se realizarán publicaciones extraordinarias de forma inmediata.
- **OCSP:** La actualización del estado del certificado en el servicio OCSP es **instantánea** tras la ejecución del proceso de emisión o revocación.

2.4 Controles de Acceso en los Repositorios

DICERT implementa controles de seguridad lógica para garantizar que los repositorios sean de **solo lectura** para el público en general. Únicamente el personal autorizado en roles de confianza (Administradores de la AC) posee permisos de escritura para actualizar las políticas y listas de revocación, protegiendo la integridad de la información mediante firmas digitales y registros de auditoría en AWS.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 Naming (Nombramiento)

3.1.1 Tipos de nombres: Los certificados de Persona Natural utilizan Nombres Distinguidos (DN) conforme al estándar X.501.

3.1.2 Necesidad de que los nombres tengan sentido: El campo *Common Name* (CN) debe contener los nombres y apellidos completos del titular según constan en su documento oficial de identidad.

3.1.3 Anonimato o seudónimos: Bajo esta PC-PN, **no se permite el anonimato ni el uso de seudónimos**. Todo certificado debe identificar de forma unívoca a una persona física real.

3.1.4 Unicidad de los nombres: Se garantiza la unicidad mediante la inclusión obligatoria del número de cédula de identidad o pasaporte en el atributo *serialNumber* del DN.

3.2 Validación Inicial de la Identidad

DICERT aplica un proceso de debida diligencia para asegurar que el solicitante es quien dice ser, empleando los siguientes métodos:

3.2.1 Prueba de posesión de la clave privada: El suscriptor debe enviar una solicitud firmada electrónicamente (**CSR**) que demuestre que posee el control exclusivo de la clave privada generada.

3.2.2 Autenticación de la identidad individual:

- **Validación Remota (Digital):** Es el método preferente. DICERT emplea un sistema de **Biometría Facial con Detección de Prueba de Vida (Liveness Detection)**. La imagen capturada en tiempo real se contrasta mediante algoritmos de IA contra la fotografía y datos biográficos almacenados en la base de datos oficial del **Registro Civil del Ecuador**.
- **Validación Documental:** El suscriptor debe cargar una imagen digital nítida de su documento de identidad vigente (cédula o pasaporte), la cual es validada mediante reconocimiento óptico de caracteres (OCR) y verificación de elementos de seguridad física.
- **Validación Presencial:** En caso de que los métodos digitales no sean concluyentes, el solicitante deberá comparecer físicamente ante un Oficial de Registro de DICERT con sus documentos originales.

3.3 Identificación y Autenticación para Solicitudes de Renovación (Re-Key)

- **Renovación de Rutina:** Si el certificado está vigente y no han variado los datos de identidad, la autenticación puede realizarse mediante la firma electrónica del propio suscriptor.
- **Límite de Tiempo:** Tras **veinticuatro (24) meses** de la validación inicial, DICERT exigirá una nueva validación biométrica completa para asegurar la vigencia de los rasgos de identidad.

3.4 Identificación y Autenticación para Solicitudes de Revocación

La solicitud de revocación debe ser autenticada de forma robusta mediante:

1. Uso del certificado digital vigente (si es accesible).
2. Validación de la **Passphrase de Revocación** única generada al momento de la emisión.
3. Validación biométrica en el portal de revocación de DICERT.

4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DEL CERTIFICADO

4.1 Solicitud de Certificado

4.1.1 Quién puede presentar una solicitud: Únicamente la persona natural interesada, de forma personal y directa. No se admiten solicitudes por medio de terceros o mandatarios, debido a la naturaleza personalísima de la firma electrónica.

4.1.2 Inscripción de la solicitud y responsabilidades: El solicitante deberá completar el formulario electrónico en el portal de DICERT, proporcionando sus datos de identidad, correo electrónico y aceptando los términos y condiciones. Es responsabilidad del solicitante la veracidad de la información y la custodia del medio donde generará sus claves.

4.2 Procesamiento de la Solicitud de Certificado

4.2.1 Realización de funciones de identificación y autenticación: La Autoridad de Registro (AR) ejecutará el protocolo de validación biométrica facial contra el Registro Civil y la validación de documentos (cédula/pasaporte) descrita en la *Sección 3.2.3.*

4.2.2 Aprobación o rechazo de solicitudes:

- **Aprobación:** Se emitirá de forma automática si la coincidencia biométrica es superior al umbral de confianza establecido (score de similitud > 90%) y los datos biométricos coinciden con la fuente oficial.

- **Rechazo:** Se notificará al usuario si existe inconsistencia documental, falla en la prueba de vida o si el documento de identidad se encuentra caducado o anulado.

4.2.3 Tiempo para procesar solicitudes: Dada la automatización en AWS, el procesamiento de solicitudes validadas por biometría se realizará en un tiempo máximo de **30 minutos**, sujeto a la disponibilidad de las bases de datos gubernamentales.

4.3 Emisión de Certificado

4.3.1 Acciones de la AC durante la emisión: Una vez aprobada la solicitud, la AC de DICERT firma el certificado utilizando su clave privada alojada en el **AWS CloudHSM**. Se vinculan los atributos del titular con la clave pública remitida en el CSR.

4.3.2 Notificación al suscriptor: El sistema envía un enlace seguro de descarga y un código de activación al correo electrónico validado del suscriptor.

4.4 Aceptación del Certificado

Se entiende que el suscriptor ha aceptado el certificado y su contenido mediante cualquiera de estas conductas:

1. Firma del Acta de Aceptación (física o digitalmente).
2. Descarga efectiva del certificado desde el repositorio seguro de DICERT.
3. El primer uso del certificado para firmar un mensaje de datos.

4.5 Uso del Par de Claves y del Certificado

4.5.1 Uso por parte del suscriptor: El suscriptor debe mantener el **control exclusivo** de su clave privada. El uso del certificado está limitado a la identificación personal y firma de documentos electrónicos.

4.5.2 Uso por parte de los terceros confiantes: Es obligación del tercero verificar la validez de la firma mediante la consulta de la CRL o el servicio OCSP de DICERT antes de otorgar validez legal al documento firmado.

4.6 Renovación de Certificados (Renewal)

DICERT no permite la renovación de certificados utilizando el mismo par de claves. Toda renovación se tratará técnicamente como una **Renovación de Claves (Re-key)** para garantizar la seguridad criptográfica.

4.7 Renovación de Claves (Re-key)

El suscriptor podrá solicitar un nuevo certificado con un nuevo par de claves antes de la expiración del actual. Si la identidad fue validada biométricamente en los últimos 24 meses, el proceso podrá ser simplificado mediante la firma electrónica del certificado vigente.

4.8 Modificación de Certificados

No se permite la modificación de los datos contenidos en un certificado emitido. Cualquier cambio en los atributos del titular (ej. cambio de apellidos) requiere la revocación del certificado actual y una nueva solicitud.

4.9 Revocación y Suspensión de Certificados

4.9.1 Circunstancias para la revocación: Compromiso de clave privada, fallecimiento del titular, o detección de errores en los datos del certificado.

4.9.2 Proceso de Revocación: La solicitud se procesará en un tiempo máximo de **dos (2) horas** tras ser validada por el portal de revocación 24/7.

4.9.3 Suspensión: Bajo esta PC-PN, **no se permite la suspensión temporal** de certificados.

4.10 Servicios de Estado del Certificado

DICERT garantiza la disponibilidad de la CRL y el servicio OCSP conforme a lo establecido en la *sección 2.3* de esta política.

4.11 Fin de la Suscripción

Ocurre por expiración del plazo de validez, revocación o solicitud de baja del servicio por parte del usuario.

4.12 Custodia y Recuperación de Claves

Está estrictamente prohibida la custodia (Escrow) de claves privadas de firma electrónica por parte de DICERT. La pérdida de la clave privada por parte del suscriptor implica la pérdida irreversible de la capacidad de firmar con ese certificado, debiendo iniciar un proceso de nueva emisión.

5. CONTROLES DE SEGURIDAD FÍSICA, DE PROCEDIMIENTOS Y DE PERSONAL

5.1 Controles de Seguridad Física

DICERT opera bajo un Modelo de Responsabilidad Compartida con Amazon Web Services (AWS).

5.1.1 Ubicación y construcción del sitio: DICERT utiliza los centros de datos de **AWS**, construidos con especificaciones industriales para resistir desastres y accesos no autorizados.

5.1.2 Acceso físico: Gestionado por AWS con múltiples capas de seguridad (biometría, guardias, CCTV). DICERT garantiza que el acceso lógico a los HSM sea solo para personal autorizado.

5.1.3 Suministro de energía y aire acondicionado: Infraestructura redundante (N+1) que asegura la operatividad ininterrumpida de los servicios de validación corporativa.

5.1.4 Exposición al agua: Instalaciones protegidas mediante sistemas de detección y drenaje de alta tecnología en las zonas de disponibilidad de AWS.

5.1.5 Prevención y protección contra incendios: Sistemas de supresión de incendios por agentes limpios que no afectan los racks de servidores.

5.1.6 Almacenamiento de medios: Los respaldos digitales se almacenan con cifrado de grado militar en múltiples regiones geográficas.

5.1.7 Eliminación de residuos: AWS destruye físicamente cualquier medio de almacenamiento retirado siguiendo el estándar NIST 800-88.

5.1.8 Respaldos fuera del sitio: Replicación automática de la base de datos de empresas y nombramientos en una región de AWS geográficamente distante.

5.2 Controles de Procedimientos

5.2.1 Roles de Confianza: Se establecen cuatro roles con privilegios segregados:

1. **Administrador de la AC:** Gestión de la plataforma.
2. **Oficial de Seguridad:** Supervisión de políticas y claves.
3. **Operador de la AC:** Emisión y revocación diaria.
4. **Auditor de Sistemas:** Revisión independiente de logs.

5.2.2 Control Mutuo (Regla de dos personas): Las operaciones críticas, como la activación del CloudHSM o la restauración de copias de seguridad de la AC, requieren la autenticación concurrente de al menos dos (2) personas en roles de confianza distintos.

5.3 Controles de Personal

5.3.1 Verificación de Antecedentes: Todo el personal de DICERT con acceso a sistemas críticos es sometido a una validación de antecedentes penales y profesionales previa a su contratación.

5.3.2 Acuerdos de Confidencialidad: La firma de acuerdos de confidencialidad (NDA) y de responsabilidad civil es obligatoria para todo el personal vinculado a la operación PKI.

5.3.3 Capacitación: Se ejecutan programas anuales de formación en ciberseguridad, gestión de AWS y normativa legal ecuatoriana de firma electrónica.

5.4 Procedimientos de Registro de Auditoría (Logs)

5.4.1 Eventos Registrados: Se registra cada solicitud, emisión, revocación, acceso fallido y cambio de configuración, tanto a nivel de aplicación como a nivel de infraestructura (AWS CloudTrail).

5.4.2 Protección de Logs: Los registros de auditoría se almacenan de forma cifrada e inmutable.

5.4.3 Retención: Siguiendo el Art. 36 de la Norma Técnica de ARCOTEL, todos los registros de auditoría se conservan por un periodo de **diez (10) años**.

5.5 Archivado de Registros

DICERT mantiene un archivo histórico digital que incluye toda la evidencia recolectada durante el proceso de validación biométrica (fotografías, coordenadas GPS del registro, resultados de coincidencia del Registro Civil). Este archivo se protege mediante **Amazon S3 Object Lock** para evitar alteraciones.

5.6 Cambio de Claves (Key Changeover)

Al menos un año antes de la expiración de la clave de la AC, se realizará una ceremonia de claves para generar una nueva jerarquía, asegurando la transición fluida para los certificados de persona natural vigentes.

5.7 Compromiso y Recuperación ante Desastres

DICERT cuenta con un Plan de Continuidad de Negocio (BCP) que permite restaurar los servicios de validación y revocación en una región distinta de AWS en un tiempo máximo (RTO) de **cuatro (4) horas** en caso de un evento catastrófico.

5.8 Terminación de la AC o RA

En caso de cese de operaciones, DICERT notificará a ARCOTEL con **90 días de anticipación** y transferirá la custodia de sus archivos y estados de certificados a la entidad que el regulador designe, garantizando la validez histórica de las firmas emitidas.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1 Generación e Instalación del Par de Claves

6.1.1 Generación del par de claves: El par de claves del suscriptor (Persona Natural) se genera bajo su **control exclusivo**. Se utiliza el método tipo:

- **Software (Archivo):** Generadas en el equipo del suscriptor mediante el uso de contenedores cifrados estándares (PKCS#12), asegurando que la clave privada nunca sea conocida por DICERT.

6.1.2 Tamaños de las claves: Se establece un tamaño mínimo de **2048 bits** para algoritmos RSA, o curvas elípticas equivalentes (NIST P-256), cumpliendo con las recomendaciones del NIST y ARCOTEL.

6.1.3 Propósitos del uso de claves: Limitados estrictamente a la firma electrónica y el no repudio, definidos en las extensiones del certificado.

6.2 Protección de la Clave Privada y Controles de Ingeniería del Módulo Criptográfico

6.2.1 Estándares del módulo criptográfico: DICERT utiliza **AWS CloudHSM** con certificación **FIPS 140-2 Nivel 3** para proteger las claves de la AC que firma estos certificados.

6.2.2 Custodia de la clave privada: Prohibida. DICERT no almacena copias de las claves privadas de los suscriptores. La responsabilidad de custodia recae íntegramente en la Persona Natural.

6.2.3 Método de destrucción de la clave privada: En caso de revocación o expiración, el suscriptor debe eliminar los archivos o formatear el dispositivo para evitar usos residuales.

6.3 Otros Aspectos de la Gestión del Par de Claves

6.3.1 Archivado de claves públicas: DICERT archiva de forma permanente las claves públicas de los suscriptores como parte del cuerpo del certificado emitido. Este archivo se mantiene por el periodo legal de **diez (10) años** para permitir la verificación histórica de firmas electrónicas, incluso después de la expiración del certificado.

6.3.2 Períodos operativos de los certificados y períodos de uso del par de claves: El período de validez para certificados de Persona Natural será de veinticuatro horas, cuarenta y ocho horas, quince días, uno (1), dos (2), tres (3) y cinco (5) años, según la solicitud del suscriptor.

- El uso de la clave privada está limitado estrictamente al periodo de vigencia del certificado. La clave pública podrá ser utilizada por terceros confiantes más allá de la vigencia únicamente para verificar firmas realizadas durante el periodo operativo.

6.4 Datos de Activación

- **6.4.1 Generación e instalación de datos de activación:** Los datos de activación (PIN o contraseña) son generados única y exclusivamente por el suscriptor al momento de la descarga o emisión.
  - DICERT impone políticas de complejidad: mínimo 8 caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales.

6.4.2 Protección de los datos de activación: El suscriptor es el único responsable de la protección y secreto de sus datos de activación.

- **Prohibición de Almacenamiento:** DICERT no almacena, conoce ni posee mecanismos de recuperación de estos datos, garantizando el principio de **control exclusivo**.

6.5 Controles de Seguridad Informática

6.5.1 Requisitos técnicos específicos: DICERT implementa controles de acceso lógico basados en el principio de "mínimo privilegio" a través de **AWS IAM**, asegurando que solo los procesos autorizados interactúen con la emisión de certificados.

6.6 Controles Técnicos del Ciclo de Vida

6.6.1 Controles de desarrollo del sistema: DICERT utiliza software de certificación de clase mundial operado en AWS. Todas las actualizaciones y parches se prueban en un entorno de *desarrollo, y otro de pruebas* antes de ser promovidos a producción.

6.6.2 Controles de gestión de la seguridad: Se aplican escaneos de vulnerabilidades mensuales y pruebas de penetración (Pentesting) anuales sobre la infraestructura de emisión.

6.7 Controles de Seguridad de Red

La infraestructura de emisión reside en una **VPC (Virtual Private Cloud)** privada en AWS, aislada de Internet. Las peticiones de los suscriptores son filtradas por un **WAF (Web Application Firewall)** y balanceadores de carga que mitigan ataques de denegación de servicio (DDoS).

6.8 Sellado de Tiempo (Time-stamping)

Los certificados y CRLs emitidos bajo esta política incorporan marcas de tiempo sincronizadas mediante el **Amazon Time Sync Service**, que utiliza una flota de relojes atómicos y satélites GPS para garantizar una precisión de nivel estrato 1 respecto al tiempo universal coordinado (**UTC**). Esto asegura que la fecha de emisión y revocación sea legalmente irrefutable.

7. PERFILES DE CERTIFICADO, CRL Y OCSP

7.1 Perfil de Certificado

DICERT emite certificados para Persona Natural bajo el estándar **ITU-T X.509 v3**, asegurando la compatibilidad con navegadores, sistemas operativos y las plataformas de la Administración Pública del Ecuador.

7.1.1 Número de versión: Se utiliza exclusivamente la **Versión 3 (v3)**. Esta versión es mandatoria para permitir la inclusión de extensiones que definen los límites de uso y la política de certificación aplicable.

7.1.2 Extensiones de los certificados: Se incluyen las siguientes extensiones para robustecer la seguridad jurídica y técnica:

- **Key Usage (Crítica):** Debe contener obligatoriamente *digitalSignature* (Firma digital), y *keyEncipherment* (Cifrado de claves).
- **Extended Key Usage (No crítica):** Incluye *clientAuth* (Autenticación de cliente) y *emailProtection* (Protección de correo).
- **Certificate Policies (No crítica):** Contiene el OID de esta PC y el enlace al repositorio.
- **Subject Alternative Name (No crítica):** Incluye la dirección de correo electrónico del suscriptor validada por la AR.
- **Authority Information Access (No crítica):** Contiene los URI para el acceso al certificado de la AC emisora y al servicio OCSP.
- **CRL Distribution Points (No crítica):** Contiene la URL pública desde donde se puede descargar la lista de revocación vigente.

7.1.3 Identificadores de objetos de algoritmos (OIDs):

- **Algoritmo de firma:** sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11).

- **Algoritmo de clave pública:** rsaEncryption (OID: 1.2.840.113549.1.1.1) con una longitud mínima de 2048 bits.

7.1.4 Formas de los nombres: Los nombres distinguidos (DN) se estructuran según la norma X.501, incluyendo:

- C=EC (País).
- O=DICERT S.A. (Organización emisora).
- OU=Firma Electrónica Persona Natural (Unidad Organizativa).
- CN= [Nombres y Apellidos del Suscriptor] (Nombre Común).
- serialNumber= [Número de Cédula o Pasaporte] (Atributo de identidad unívoco).

7.1.5 Restricciones de nombres: No se imponen restricciones de nombres adicionales a las establecidas por el estándar X.500. No se permiten nombres anónimos o seudónimos.

7.1.6 Identificador de objeto (OID) de la política de certificado: El OID que identifica unívocamente a este perfil de Persona Natural es: **1.3.6.1.4.1.62486.2.1.1**.

7.1.7 Uso de la extensión de restricciones de política: Esta extensión no se utiliza en los certificados de suscriptor final.

7.1.8 Sintaxis y semántica de los calificadores de política: Se incluye el calificador id-qt-cps, el cual contiene un puntero (URL) hacia la Declaración de Prácticas de Certificación (DPC) de DICERT disponible en su repositorio oficial.

7.1.9 Semántica de procesamiento para la extensión de Políticas de Certificado crítica: La extensión *Certificate Policies* se marca como **no crítica**, permitiendo que aplicaciones que no reconozcan el OID de DICERT puedan seguir procesando la cadena de confianza básica del certificado.

7.2 Perfil de la CRL

7.2.1 Número de versión: DICERT emite Listas de Revocación de Certificados en **Versión 2 (v2)**, conforme a la RFC 5280.

7.2.2 Extensiones de la CRL y de las entradas de la CRL:

- **Authority Key Identifier:** Para identificar la clave privada de la AC que firmó la lista.
- **CRL Number:** Un número secuencial no repetitivo para cada CRL emitida.
- **Reason Code:** Indicando el motivo de la revocación (ej. *keyCompromise*, *cessationOfOperation*).

7.3 Perfil OCSP

7.3.1 Número de versión: El servicio de respuesta en línea cumple con la **Versión 1 (v1)** bajo los lineamientos de la RFC 6960.

7.3.2 Extensiones OCSP: Se soporta y recomienda el uso de la extensión *Nonce* para asegurar la frescura de la respuesta y evitar ataques de repetición en las consultas de estado.

8. AUDITORÍA DE CUMPLIMIENTO Y OTROS CONTROLES

8.1 Frecuencia y circunstancias de la evaluación

DICERT se somete a una auditoría de cumplimiento técnico y legal con una **periodicidad anual**, de conformidad con lo establecido en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y las Normas Técnicas vigentes de **ARCOTEL**.

- **Evaluaciones Extraordinarias:** Se realizarán auditorías adicionales ante cambios significativos en la arquitectura técnica (v.gr., cambios en la configuración del AWS CloudHSM o migraciones de infraestructura crítica) o cuando el ente regulador así lo disponga en ejercicio de sus facultades de control.

8.2 Identidad y cualificaciones del evaluador

La auditoría de cumplimiento debe ser ejecutada por una firma auditora externa e independiente, con capacidad técnica comprobada en la evaluación de infraestructuras de clave pública (PKI).

- **Requisitos del equipo auditor:** Los evaluadores deberán contar con certificaciones profesionales de reconocimiento internacional (tales como **CISA**, **CISM**, o auditores calificados bajo estándares **WebTrust** o **ETSI**).
- **Registro:** La firma auditora deberá cumplir con los requisitos de registro o calificación que ARCOTEL exija para auditar a Entidades de Certificación en el Ecuador.

8.3 Relación del evaluador con la entidad evaluada

Para garantizar la objetividad y transparencia del proceso, el auditor debe mantener una **independencia absoluta** respecto a DICERT.

- No podrá existir relación de propiedad, parentesco, ni conflictos de intereses comerciales o financieros entre los socios y personal de la firma auditora y los directivos o personal en roles de confianza de DICERT.
- El auditor no podrá haber participado en el diseño, implementación o administración de los sistemas que son objeto de la evaluación.

8.4 Temas cubiertos por la evaluación

La auditoría evaluará el cumplimiento de DICERT respecto a la Declaración de Prácticas de Certificación (DPC) y esta Política de Certificados (PC-PN), cubriendo:

1. **Integridad Técnica:** Gestión de las claves de la AC dentro de AWS CloudHSM y seguridad de la red VPC.
2. **Procesos de Identificación:** Verificación de la eficacia de los métodos de **biometría facial** y cotejo contra el Registro Civil.
3. **Gestión de Operaciones:** Correcta aplicación de los quórums de seguridad (regla de dos personas) y segregación de funciones.
4. **Gestión Documental:** Integridad y retención de expedientes y registros de auditoría por el plazo de 10 años.
5. **Respuesta a Incidentes:** Eficacia de los planes de continuidad del negocio y recuperación ante desastres en la nube.

8.5 Acciones tomadas como resultado de una deficiencia

En caso de que el informe de auditoría identifique hallazgos, observaciones o no conformidades:

- **Plan de Acción:** El Oficial de Seguridad de DICERT elaborará un Plan de Acción Correctiva (PAC) en un plazo no mayor a **quince (15) días laborables**.
- **Remediación:** Los hallazgos calificados como "críticos" deberán ser subsanados de forma inmediata. Las deficiencias menores se corregirán dentro de los cronogramas aprobados por la Gerencia General.
- **Seguimiento:** El auditor verificará la implementación de las medidas correctivas en una visita de seguimiento o en la auditoría del periodo subsecuente.

8.6 Comunicación de resultados

Los resultados de la auditoría de cumplimiento serán comunicados de la siguiente manera:

- **Interna:** El informe final será entregado a la Gerencia General y al Oficial de Seguridad para la toma de decisiones estratégicas.
- **Externa:** Una copia íntegra del informe, junto con el dictamen del auditor, será remitida formalmente a **ARCOTEL** dentro de los términos legales establecidos para el mantenimiento del registro de la entidad.
- **Pública:** DICERT podrá publicar un "Sello de Cumplimiento" o una carta de conformidad del auditor en su repositorio web, sin comprometer información técnica sensible que pueda afectar la seguridad de la infraestructura.

9. OTRAS DISPOSICIONES COMERCIALES Y LEGALES

9.1 Tarifas

9.1.1 Tarifas de emisión o renovación de certificados: DICERT establece sus tarifas basándose en las condiciones del mercado y la modalidad de validación (biométrica remota o presencial). Las tarifas vigentes se publican de forma transparente en el portal web oficial.

9.1.2 Tarifas de acceso al certificado: El acceso a los certificados públicos para verificación es gratuito.

9.1.3 Tarifas de información sobre el estado de revocación: Las consultas a través de CRL y OCSP son gratuitas y de libre acceso para cualquier tercero confiante.

9.1.4 Tarifas por otros servicios: Servicios adicionales como el soporte técnico personalizado o integración de APIs se rigen por contratos de servicios específicos.

9.1.5 Política de reembolsos: Se contempla el reembolso únicamente por fallos técnicos imputables a la infraestructura de DICERT dentro de los primeros 5 días laborables tras la emisión, siempre que el certificado no haya sido utilizado.

9.2 Responsabilidad Financiera

9.2.1 Cobertura de seguro: DICERT mantiene las garantías financieras y pólizas de responsabilidad civil exigidas por ARCOTEL para cubrir posibles perjuicios derivados de su actividad como Entidad de Certificación.

9.2.3 Cobertura de seguro para las entidades finales: No se ofrece un seguro de garantía individual al suscriptor, salvo pacto en contrario mediante un servicio premium.

9.3 Confidencialidad de la Información Comercial

9.3.1 Alcance de la información confidencial: Incluye los registros de auditoría detallados, planes de seguridad, claves privadas de la AC y cualquier dato técnico del CloudHSM.

9.3.2 Información que no se considera confidencial: Los certificados emitidos, las CRLs, esta PC y la DPC son de naturaleza pública.

9.3.3 Responsabilidad de proteger la información confidencial: DICERT aplica el principio de "necesidad de conocer" y acuerdos de confidencialidad estrictos con todo su personal.

9.4 Privacidad de la Información Personal

9.4.1 Plan de privacidad: DICERT se adhiere a la **Ley Orgánica de Protección de Datos Personales (LOPDP)**.

9.4.2 Información tratada como privada: Datos biométricos, direcciones domiciliarias, números telefónicos y copias de documentos de identidad no contenidos en el certificado.

9.4.3 Información no privada: Datos visibles en el certificado (RUC, Nombre).

9.4.4 Responsabilidad de protección: Cifrado de datos en AWS S3 y acceso restringido por roles.

9.4.5 Notificación y consentimiento: El suscriptor otorga su consentimiento expreso al momento de la solicitud para el tratamiento de sus datos con fines de validación de identidad.

9.4.6 Divulgación por procesos judiciales: DICERT solo entregará información privada bajo orden judicial motivada o requerimiento legal de autoridad competente.

9.5 Derechos de Propiedad Intelectual

DICERT es titular exclusivo de los derechos de autor sobre esta PC, los OIDs asignados y el software de interfaz de usuario. El suscriptor posee el derecho de uso sobre su certificado durante la vigencia del mismo.

9.6 Representaciones y Garantías

9.6.1 Garantías de la AC: DICERT garantiza que el proceso de validación biométrica cumple con los estándares de seguridad para asegurar que el certificado pertenece a la persona identificada.

9.6.2 Representaciones y Garantías de la AR (Autoridad de Registro): Las oficinas o sistemas de registro, sean propios de DICERT o delegados, garantizan que la identificación del solicitante se realizó mediante el cotejo de identidad con la base de datos oficial del **Registro Civil del Ecuador**, se han recolectado y custodiado las evidencias de identidad (biometría, fotos, documentos) de forma íntegra y confidencial, que no existen errores de transcripción en los datos enviados a la AC para la generación del certificado; y que el personal que opera la AR cumple con los roles de confianza y ha superado las pruebas de idoneidad.

9.6.3 Garantías de los suscriptores: El suscriptor garantiza la veracidad de la información proporcionada y asume la responsabilidad total por el uso y custodia de su clave privada.

9.6.4 Representaciones y Garantías de las Partes Confiantes (Terceros): Cualquier tercero que confíe en una firma electrónica de DICERT garantiza que ha verificado la validez de la

cadena de confianza hasta la AC Raíz de DICERT, y ha consultado el estado de revocación del certificado a través de la CRL o el servicio OCSP al momento de la validación.

9.6.5 Representaciones y Garantías de Otros Participantes: Los proveedores de servicios críticos (como AWS para la infraestructura de nube o proveedores de motores biométricos) garantizan a DICERT la continuidad y seguridad de sus servicios mediante acuerdos de nivel de servicio (SLA) y certificaciones internacionales de seguridad (SOC 2, ISO 27001), los cuales son supervisados por el Oficial de Seguridad de DICERT.

9.7 Descargo de Responsabilidad de Garantías

DICERT no se responsabiliza por la idoneidad del certificado para usos no especificados en la sección 1.4 de esta política.

9.8 Limitaciones de Responsabilidad

Salvo en casos de negligencia grave o dolo comprobado por parte de DICERT, la responsabilidad total de la entidad frente al suscriptor o terceros está limitada al valor pagado por el certificado o al monto máximo establecido en la póliza de seguros ante ARCOTEL.

9.9 Indemnizaciones

El suscriptor indemnizará a DICERT por cualquier daño, reclamo o gasto derivado de la falsedad en sus datos o el descuido en la custodia de su clave privada que resulte en un perjuicio a terceros.

9.10 Vigencia y Terminación

9.10.1 Plazo de vigencia: Esta política entra en vigor tras su aprobación y registro ante ARCOTEL.

9.10.2 Terminación: La vigencia cesa con la publicación de una versión superior.

9.11 Comunicaciones Individuales

Las comunicaciones oficiales se realizarán a través del correo electrónico registrado por el suscriptor en el proceso de solicitud.

9.12 Enmiendas

Cualquier cambio sustancial en esta PC será notificado a ARCOTEL con al menos 15 días de antelación a su publicación.

9.13 Disposiciones sobre Resolución de Disputas

Toda controversia derivada de la interpretación o aplicación de esta política será resuelta mediante **Arbitraje en Derecho** en el Centro de Arbitraje y Mediación de la Cámara de Comercio de **Quito**.

9.14 Ley Aplicable

Esta política se rige íntegramente por las leyes de la **República del Ecuador**.

9.15 Cumplimiento con la Ley Aplicable

DICERT garantiza que su operación en la nube (AWS) no vulnera la soberanía de los datos de los ciudadanos ecuatorianos.

9.16 Disposiciones Diversas

Si una autoridad judicial declara nula alguna sección de esta PC, las demás secciones mantendrán su plena vigencia y efecto.

10. Control de Cambios

POLÍTICA DE CERTIFICADOS PARA PERSONA NATURAL (PC-PN)						
CÓDIGO: PCPN-DES-DC-0019					**CLASIFICACIÓN:** Documento de Acceso Público	
VERSIÓN	**DETALLE**	**ELABORADO POR:**	**FECHA APRUEBA**	**REVISADO POR:**	**FECHA PUBLICACIÓN**	**LOCALIZACIÓN**
1.0	Versión Inicial	Sebastián Poveda	05/02/2026	Galo Becerra	05/02/2026	https://dicert.com.ec/links/dpc

11. Firmas de Responsabilidad

Aprobado por:	**Firma**
Nombre: Galo Becerra Cargo: Gerente General	Digitally signed by GALO SANTIAGO BECERRA GORDÓN

Elaborado por:	**Firma**
Nombre: Sebastián Poveda Cargo: Encargado Seguridad de la Información	1750559476 SEBASTIAN LEONARDO POVEDA VALLADARES Digitally signed by 1750559476 SEBASTIAN LEONARDO POVEDA VALLADARES Date: 2026.03.02 15:19:12 -05'00'