Certificamos Información Digital

DOCUMENTACIÓN MECANISMOS DE SEGURIDAD	
SGSI - GG	Código: **DMS-DC-GG-009**
	Versión: 3.0
	Clasificación de Información: **Documento Confidencial**

DOCUMENTACIÓN MECANISMOS DE SEGURIDAD

Aprobado por:	**Firma de Aprobación:**
Galo Becerra	Digitally signed by GALO SANTIAGO BECERRA GORDÓN
	Fecha de Aprobación: 22 de enero de 2026

Contenido / Índice

Control de Cambios

VERSIÓN	DETALLE	ELABORADO POR:	FECHA APROBACIÓN	REVISADO POR:
1.0	Versión Inicial	Sebastian Poveda	30-10-2024	Galo Becerra
2.0	Revisión ARCOTEL	Sebastián Poveda	08-04-2025	Galo Becerra
3.0	Revisión Interna	Sebastián Poveda	22-01-2026	Galo Becerra

DOCUMENTOS DE SOPORTE DE LAS MEDIDAS DE SEGURIDAD

El presente documento contiene el detalle de los mecanismos de seguridad que se implementan en DICERT para: 1) evitar la falsificación de certificados; 2) precautelar la integridad y resguardo de documento; 3) protección contra siniestros; 4) control de accesos y confidencialidad durante la generación de claves; 5) la descripción de sistemas de seguridad; 6) estándares de seguridad; y, 7) sistemas de respaldo.

De manera complementaria se deberá revisar el documento Diagrama Técnico de Cada Nodo o Sitio Seguro para un entendimiento completo de las medidas que se implementan en DICERT.

I. MECANISMOS DE SEGURIDAD

1.1. Seguridad a través de la criptografía

La criptografía ofrece seguridad de privacidad de mensajes a través de una o varias llaves. Existen llaves simétricas y asimétricas, esta última utiliza dos llaves, una pública y otra privada. La primera es la llave a la que cualquier entidad puede tener acceso, mientras la llave privada solo el titular la puede utilizar. Esto es llamado criptografía de llave pública y privada.

La llave privada se utiliza para firmar los mensajes y la llave pública para verificar la firma. La principal ventaja de este método es la libre distribución de llaves públicas.

1.2. Certificado digital

El certificado digital es creado a partir de la llave privada generada por el sistema. Este garantiza la identidad de una persona y permite la firma electrónica de documentos. Quien recibe un documento firmado digitalmente tiene la garantía de que el documento es el documento original y no ha sido manipulado en el proceso de envío. Así mismo, quien firme el documento no puede negar la autoría de la firma (no repudio).

El certificado digital contiene la llave pública e información del titular del certificado. Esto viene acompañado de la firma de la entidad de certificación (Autoridad de Certificación o CA), que es

la entidad de confianza que asegura que los datos del titular son correspondientes con la llave pública.

1.3. Entidad de certificación

La entidad de certificación que se dispone es AWS (Amazon Web Services) AC Privada. Esta plataforma garantiza un servicio de alta disponibilidad, crear jerarquías de AC, y una API para gestionar los certificados desde la programación del módulo de gestión de certificados digitales.

La AC Privada de AWS es una entidad de certificación privada segura y permite administrar autoridades de certificado de forma centralizada.

La entidad de certificación, por tanto, es administrada por AWS. Así mismo, se tiene una administración integrada del ciclo de vida de los certificados, un almacenamiento seguro de llaves con respaldo en HSM (módulos de seguridad de hardware) para las llaves de la AC (cumpliendo con las normas de seguridad FIPS 140-2 Nivel 3) y auditoría y registro de los eventos de la AC. Adicionalmente se tiene una integración de IAM (Identity and Access Management) de AWS para administrar las políticas de acceso a la CA.

1.4. Algoritmo RSA

El algoritmo RSA es utilizado con el par de llaves pública y privada. Es un algoritmo asimétrico. Al realizarse el envío de un mensaje, quien lo envía utiliza la llave pública para cifrar el mensaje y el receptor utiliza su llave privada para leer el mensaje. El algoritmo RSA convierte los mensajes enviados en números y su funcionamiento está basado en el producto de dos números primos, grandes, mayores que 10.100, elegidos aleatoriamente para generar la clave de descifrado. Es un algoritmo seguro ya que no existen formas rápidas actualmente para factorizar un número así de grande en sus factores primos.

Para más información técnica sobre el algoritmo RSA se puede consultar la siguiente página:
https://tools.ietf.org/html/rfc8017

1.5. Algoritmo SHA

El algoritmo SHA (Secure Hash Algorithm) es una función hash criptográfica que tiene una longitud de 256 bits. Esta función no utiliza llave, lo que significa que es un código de detección de manipulación.

Es decir, el uso de este algoritmo garantiza la inmutabilidad de la información enviada utilizando los certificados digitales generados con la herramienta.

Para más información técnica sobre el algoritmo SHA se puede consultar la siguiente página:

https://tools.ietf.org/html/rfc4634

1.6. Procedimientos de generación de claves

Los procesos de generación de claves se ejecutan bajo estrictos controles de seguridad que cumplen con las normas ISO/IEC 15408 y ISO/IEC 27001, garantizando la inalterabilidad y autenticidad de las claves generadas.

Todas las claves criptográficas son creadas y gestionadas dentro de módulos de seguridad de hardware (HSM) certificados bajo el estándar FIPS 140-2 Nivel 3, lo que asegura su protección contra manipulaciones y acceso no autorizado. Estos procedimientos están alineados con las mejores prácticas internacionales de seguridad.

1.7. Manual de Uso y Gestión de Claves Criptográficas

DICERT implementa un *Manual de Uso y Gestión de Claves Criptográficas* que regula el ciclo de vida completo de las claves utilizadas en sus servicios de certificación, siguiendo el lineamiento de administradores como *AWS-KMS*. Este manual cubre los procedimientos de generación, distribución, almacenamiento, renovación y destrucción segura de las claves criptográficas, garantizando su integridad y confidencialidad en todo momento. Además, establece políticas de control de acceso basadas en roles y responsabilidades para que sólo el personal autorizado gestione y acceda a las claves; asimismo, define mecanismos de auditoría y monitoreo continuo para asegurar el cumplimiento con los más altos estándares de seguridad, en cumplimiento de las normativas vigentes.

1.8. Política de Seguridad de la Información

DICERT ha implementado una Política de Seguridad de la Información para proteger la **integridad, confidencialidad y disponibilidad** de la información gestionada en sus sistemas. Esta política establece controles de acceso estrictos, procedimientos de monitoreo continuo y mecanismos de respuesta ante incidentes de seguridad. Asimismo, define los roles y responsabilidades del personal en la gestión segura de la información y requiere auditorías regulares para verificar el cumplimiento de los estándares de seguridad, asegurando la protección integral de los datos y activos de información en conformidad con la normativa vigente.

Acceder al link de la Política de SGSI de DICERT.
https://h2o.ac/k1GeLgI8rV o consultar Anexo de la Política.

1.9. Política de Protección de Datos

DICERT ha implementado una Política de Protección de Datos para salvaguardar la información personal ingresada al sistema. Esta política establece estrictos deberes de confidencialidad en el manejo de los datos y la obligación de mantener registros de auditoría sobre las consultas realizadas a los certificados emitidos. Además, asegura la protección adecuada de los derechos y libertades de los titulares de datos personales, en estricto cumplimiento con la normativa legal vigente.

Acceder al link de la Política de Protección de Datos Personales de DICERT.
https://h2o.ac/YjOrit2a7T o Consultar Anexo de la Política

II. CONDICIONES DE MANEJO DE LA INFORMACIÓN PROPORCIONADA POR LOS USUARIOS

2.1 Almacenamiento de información.

Mientras el usuario haga uso de los servicios de DICERT su información debe ser conservada. Si un usuario deja de utilizar los servicios de DICERT, ésta conservará de manera segura su información por el tiempo que señale la ley para la prescripción de acciones que por daños puedan iniciarse, con la única finalidad de contar con la información y poder proporcionarla, de ser el caso, en cualquier controversia o litigio posterior, derivados de los servicios, documentos o el uso de éstos.

Si un usuario solicita la eliminación de su información durante el periodo de vigencia en que DICERT le está prestando un servicio y la prestación del servicio depende del mantenimiento y conservación de dicha información, entonces se entenderá que el usuario desea terminar anticipadamente la prestación del servicio sin lugar a reclamo posterior alguno y sin derecho a la devolución de valor alguno que haya pagado por tal servicio, cuya terminación anticipada está solicitando en virtud de la eliminación de su información; ocurrido lo anterior DICERT conservará la información de manera segura con la única finalidad de contar con la información y poder proporcionarla, de ser el caso, en cualquier controversia o litigio posterior, derivados de los servicios, documentos o el uso de éstos; y comenzará a transcurrir el tiempo que señale la ley para la prescripción de acciones que por daños puedan iniciarse y que será igual al tiempo de conservación de la información por parte de DICERT.

2.2. Información que se comparte y autorización del usuario para el efecto

DICERT entiende la naturaleza sensible de la información personal y en consecuencia la información que el usuario provee a DICERT estará protegida y no será compartida con terceros no relacionados, en los términos establecidos por la ley.

A pesar de que DICERT no comparte la información personal con terceros no relacionados, el usuario puede explícitamente indicar que información no desea que sea compartida en el futuro a través del envío de una solicitud al correo electrónico soporte@dicert.com.ec. DICERT cumplirá con su solicitud dentro de los plazos establecidos en la Ley, salvo que exista una excepción legal que nos impida hacerlo; en cuyo caso se informará de la misma. Si un usuario solicita no compartir su información durante el periodo de vigencia en que DICERT le está prestando un servicio y la prestación del servicio depende de la compartición de dicha información, entonces se entenderá que el usuario desea terminar anticipadamente la prestación del servicio sin lugar a reclamo posterior alguno y sin derecho a la devolución de valor alguno que haya pagado por tal servicio, cuya terminación anticipada está solicitando en virtud de la no compartición de su información.

No obstante lo anterior, existen circunstancias en las que DICERT puede o debe compartir su información para propósitos específicos:

- A terceros incluyendo, pero sin limitarse a empresas asociadas o filiales de la Compañía solamente para los propósitos establecidos en esta Política de Seguridad.
- A nuestros proveedores de servicios quienes están obligados según la ley a proteger su información y solamente utilizarla de acuerdo con nuestras instrucciones.
- Para fines de almacenamiento seguro. Para lo cual el usuario autorizará expresamente la transferencia internacional de sus datos a las entidades proveedoras de almacenamiento, contratadas por DICERT para el efecto.
- A entidades gubernamentales y departamentos corporativos para propósitos de auditoría o cumplimiento cuando sea necesario.
- A autoridades judiciales o gubernamentales cuando sea requerido por la ley a través de una orden judicial ya sea dentro del territorio nacional o en el exterior.
- Para cumplir con la normativa vigente que exige la publicación y entrega de reportes periódicos a la autoridad nacional competente, de listas de extinción, revocación, y suspensión de los certificados de firma electrónica.

DICERT puede compartir datos demográficos que no contienen información de identificación personal.

El usuario expresará su consentimiento libre, específico, informado e inequívoco, autorizando para que sus datos puedan ser transferidos/compartidos a cualquier tercero relacionado a DICERT , y utilizados por éstos, incluyendo, pero sin limitarse a proveedores, empresas asociadas o filiales de la Compañía.

2.3 Declaración del Usuario

En el contrato a ser suscrito por el usuario, el usuario de manera expresa declarará que ha leído y comprendido la Declaración de Prácticas de Certificación, Políticas de Certificación de DICERT, los Términos y Condiciones de DICERT y el contenido total del contrato, por lo que los acepta de manera voluntaria y presta su consentimiento expreso e inequívoco de regirse por los mismos.

III. CONTENEDORES CRIPTOGRÁFICOS

El contenedor criptográfico utilizado en el sistema es el Almacén de Llaves (Keystore en inglés). Este es un contenedor de llaves privadas y certificados digitales, el cual debe ser descargado como un archivo por el titular del certificado digital. El certificado que se guarda en el Almacén de Llaves utiliza el formato PKCS#7 ya firmado por la AC. Inicialmente este contenedor se crea con un certificado inicial en formato PKCS#10, siendo este un CSR (solicitud de firma de certificado) para posteriormente registrar el certificado en la AC y obtener así el certificado digital firmado.

IV. ESTÁNDARES Y NORMAS INTERNACIONALES

Los servicios de AWS utilizados cumplen con normas internacionales de seguridad, tales como ISO 27001 para gestión de la seguridad de la información, PCI DSS para protección de datos de pagos, y FIPS 140-2 Nivel 3 para seguridad criptográfica en HSM. Estas certificaciones aseguran que los procesos cumplen con las mejores prácticas y estándares internacionales aplicables a la gestión de información y seguridad de datos.

4.1. Norma ISO/IEC 9594-8 estándar x.509

Cumpliendo con la norma ISO/IEC 9594-8 y el estándar x.509, se tienen los siguientes campos obligatorios en el certificado:

- Datos del certificado:
  - Versión
  - Número de serie
  - Emisor del certificado
  - Validez (fecha de inicio y fecha final de validez)
  - Nombre distinguido del sujeto
  - Llave pública del sujeto

- Firma del Certificado:
  - Algoritmo de firma
  - Firma del certificado

De forma obligatoria, se maneja la extensión KeyUsage, especificando los posibles usos del certificado. Inicialmente se utiliza solamente el valor *DigitalSignature* para la firma electrónica de documentos.

Adicionalmente, se manejan de manera opcional las siguientes extensiones:

AuthorityKeyIdentifier: Identificador de un certificado de llave pública de la AC asociado con la llave privada usada para firmar el certificado.

Certificate Policies: Especifica la política de certificación que la AC cumple para emitir certificados.

La versión de los certificados es X.509 versión 3.

4.2. RFC 2560 – x.509 infraestructura de llave pública internet. PKI protocolo en línea del estado del certificado – OCSP (Online certificate status protocol)

El protocolo de estado de certificado en línea (OCSP) se puede utilizar para cumplir con requisitos operativos relacionados con la información de revocación de una manera más oportuna de lo que es posible con las CRL.

Las Listas de Certificados Revocados (CRL) se actualizan diariamente y se publican en una plataforma accesible al público, permitiendo que los usuarios puedan verificar de inmediato el estado de cualquier certificado. Esta práctica garantiza transparencia y seguridad en la gestión de los certificados digitales.

Las respuestas OCSP son por defecto de la versión 0 (equivalente de la versión v1). Las posibles extensiones que puede tener una respuesta OCSP son las siguientes:

Nonce: Vincula criptográficamente una solicitud y una respuesta, siendo identificado por el objeto: id-pkix-ocsp-nonce OBJECT IDENTIFIER:: = {id-pkix-ocsp 2}

CRL References: Utilizadas para que el OCSP indique la CRL en la que se encuentra un certificado revocado como un mecanismo de auditoría. El identificador de esta extensión es: id-pkix-ocsp-crl OBJECT IDENTIFIER:: = {id-pkix-ocsp 3}

En cumplimiento con la norma RFC 2560 – x.509 los datos de solicitud de OCSP son los siguientes:

- Versión de protocolo
- Solicitud de servicio
- Identificador del certificado objetivo
- Extensiones opcionales que pueden ser procesadas por el OCSP

Al recibir una solicitud, el servidor OCSP determina si el mensaje está formado correctamente, si el servidor está configurado para proveer el servicio solicitado y que la solicitud contiene la información requerida. En caso de que alguna de estas condiciones falle, el servidor produce un mensaje de error.

Como base, una respuesta OCSP está compuesto por los siguientes campos:

- Versión de la sintaxis de respuesta
- Nombre de quien responde
- Respuestas para cada uno de los certificados en la solicitud
- Extensiones opcionales
- Algoritmo de firma OID
- Firma computada utilizando el hash de la respuesta

Así mismo, la respuesta para cada uno de los certificados en una solicitud consiste en los siguientes campos:

- Identificador del certificado objetivo
- Estado del certificado
- Intervalo de validez de la respuesta
- Extensiones opcionales

V. COMPONENTES DE SEGURIDAD PERIMETRAL

5.1. Sistema de prevención de intrusos IPS

Una ventaja de la infraestructura de AWS es la facilidad para habilitar servicios bajo demanda, en el caso de detección y prevención de intrusos AWS ofrece los servicios que se detallan a continuación.

Amazon CloudWatch

Su objetivo es recolectar y almacenar logs de otros servicios de AWS y de la aplicación, tales logs incluyen logs de Amazon Route 53, Amazon VPC Flow Logs, Amazon CloudTrail, entre otros servicios.

Adicionalmente recolecta los logs de los microservicios de la plataforma de firmas digitales. También realiza la recolección de métricas tales como uso de CPU, uso de disco, actividad de usuario, entre otros.

La información recolectada es utilizada para generar paneles de monitoreo y alertas personalizadas. De esta manera un administrador cuenta con información valiosa para tomar acciones según el nivel de prioridad. Por ejemplo, el análisis de logs permite determinar accesos en horarios que no son regulares, nuevos usuarios que realizan cambios en la infraestructura, etc.

La plataforma de firmas digitales utiliza este servicio para monitoreo y detección de intrusos.

Amazon Inspector

Este servicio es un evaluador de seguridad de las instancias de servidor y aplicaciones, cuyo fin es reportar y prevenir posibles riesgos de seguridad. La evaluación consiste en analizar exposiciones, vulnerabilidades y desviaciones de buenas prácticas.

Para este propósito cuenta con paquetes de reglas pre-definidas, las mismas que se basan en buenas prácticas de seguridad y definiciones de vulnerabilidad. Estas reglas son actualizadas constantemente por Amazon.

Amazon GuardDuty

Se trata de un servicio que hace uso del aprendizaje de máquina para detectar posibles amenazas mediante el análisis de eventos generados en servicios como AWS CloudTrail, Amazon VPC Flow Log y DNS Logs. Por ejemplo, las posibles amenazas que este servicio identifica son: llamadas inusuales a APIs, comunicación con direcciones IP consideradas como maliciosas, accesos a los recursos de AWS desde ubicaciones geográficas inusuales, intentos de deshabilitar logs, entre otros.

Control de Acceso y Autenticación: Los sistemas de control de acceso y autenticación utilizan mecanismos de autenticación multifactoriales (IAM y AWS Cognito), con acceso basado en roles (RBAC) que permite asignar permisos específicos a usuarios y administradores. Cada acceso se audita y se monitorea para detectar actividades

sospechosas. Estas políticas garantizan que sólo personal autorizado puede acceder a los sistemas críticos.

5.2. Firewall

Como parte de la arquitectura de red (ver sección 1.1 Descripción del esquema de red en el documento denominado DIAGRAMA TÉCNICO DE CADA NODO O SITIO SEGURO) se establece un Grupo de Seguridad de la VPC.

El Grupo de Seguridad actúa como un firewall virtual de cada instancia EC2 que forma parte de la VPC, este permite el control del tráfico de entrada y salida mediante la configuración de reglas.

Entre las principales características del Grupo de Seguridad están:

- Manejo de reglas de entrada y salida.
- Los Grupos de Seguridad están asociados a las interfaces de red de las instancias de servidor.
- Por defecto, una interface de red está asociada con el Grupo de Seguridad definido en la VPC.
- Las reglas pueden ser definidas utilizando IPs, puertos, protocolos y otros Grupos de Seguridad.

5.3. Balanceadores

Se utiliza un Balanceador de Carga de Red que se gestiona a través del servicio Amazon ELB (Elastic Load Balancing). Este balanceador se configura por Zona de Disponibilidad y controla el tráfico TCP y UDP para direccionar hacia el objetivo destino.

Los tiempos de latencia del balanceador de carga de red son extremadamente cortos y soporta conexiones TCP de larga duración, lo cual facilita el uso de WebSockets.

VI. ESQUEMA DE SEGURIDAD PERIMETRAL

Nivel de Periferia

- Visitantes mediante acceso mediante autorización
- Trabajadores mediante acceso autorizado y escudriñado constantemente
- Acceso limitado a áreas pre-aprobadas y mediante autenticación de múltiple factor

- Monitoreo mediante cámaras
- Uso de sistemas de detección de intrusos
- Uso de sistemas de monitoreo de logs de acceso

Nivel de Infraestructura

- Revisión de autorización de acceso al nivel
- Diagnósticos de máquinas, redes y equipos de respaldo
- Chequeos rutinarios de mantenimiento
- Equipamiento de respaldo en caso de emergencia (agua, energía, telecomunicaciones y conectividad a internet)
- Control de temperatura y humedad

Nivel de Datos

- Revisión de autorización de acceso al nivel
- Sistemas de detección de intrusos y lanzamiento de alertas por actividad inusual o sospechosa
- Cámaras de seguridad
- Dispositivos de acceso que requieren autenticación de factor múltiple
- Notificación de intento de remoción de datos
- Estándares para instalación, servicio y destrucción de dispositivos de almacenamiento
- AWS es auditado por auditores externos para cumplir con más de 2600 requerimientos durante el año

Nivel Ambiental

- Dispositivos de detección de agua y fuego, así como equipos para reducir el riesgo y notificar al personal de AWS
- Cada Región AWS tiene múltiples Zonas de Disponibilidad donde cada zona consiste de uno o más centros de datos que están físicamente separados uno de otro, y tienen redundancia de energía y red de comunicaciones.
- Plan de Continuidad de Negocio de AWS como guía ante posibles desastres naturales.

VII. ESQUEMA DE SEGURIDAD DE LA INFRAESTRUCTURA DE LLAVE PÚBLICA PKI

La infraestructura de PKI cumple con los lineamientos de seguridad de Amazon expuestos en el siguiente link:
https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

Como medidas de seguridad de la AC Privada de AWS, se tiene en consideración la protección de los datos, la gestión de acceso, logs, monitoreo y seguridad de la infraestructura, en cumplimiento de las normativas ISO 27001/27017, PCI DSS y FIPS 140-2.

En el siguiente link se pueden revisar los detalles de la seguridad en el servicio de la AC Privada de AWS: https://docs.aws.amazon.com/acm-pca/latest/userguide/security.html

Por otro lado, en la aplicación se tienen en consideración las medidas que se describen en los apartados siguientes.

VIII. PLAN DE CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN ANTE DESASTRES

DICERT opera sobre una plataforma en la nube que brinda respuesta eficiente ante desastres, permitiendo centrarse en las funciones relevantes de recuperación. Los servicios en la nube ofrecen altos niveles de disponibilidad y aseguran la continuidad del negocio en caso de que una incidencia sea detectada en la plataforma de hardware.

Entre los aspectos para el plan de contingencia, en caso de que sea necesario, se consideran los siguientes:

- **Restauración de conectividad**: Soporte técnico especializado que forma parte del plan ofrecido por el proveedor de la nube.
- **Mapeo de incidentes**: Coordinación rápida y ágil para que los servicios de emergencia puedan completar sus tareas de forma local y dirigir recursos.
- **Recuperación regional**: En caso de falla general de una región de AWS, se cuenta con mecanismos de restauración de la infraestructura de la plataforma de firmas electrónicas en otra región mediante scripts (infrastructure as code).
- **Redundancia de software**: A nivel de software, se cuenta con funciones de contingencia que permiten llevar a cabo operaciones manuales cuando los servicios de terceros (por ejemplo, Registro Civil o Reconocimiento Facial) no están disponibles.

El plan de continuidad de negocio está respaldado por pruebas periódicas que incluyen simulaciones de diferentes escenarios críticos, con protocolos (detalles operativos) para cada fase de un incidente (antes, durante y después).

Este esquema cumple con la norma ISO 22301, que establece prácticas de continuidad del negocio para minimizar la interrupción de servicios críticos y proteger la disponibilidad de la información.

IX. SISTEMA DE CONTROL DE ACCESO AL CENTRO DE CÓMPUTO

El proveedor de la nube otorga acceso físico a su centro de datos sólo a empleados autorizados.

En caso de requerir acceso, es necesario solicitarlo proporcionando la siguiente información:

- Una justificación empresarial clara y válida.
- Especificar a qué capa del centro de datos requiere acceso la persona.
- Tiempo de acceso.

Las solicitudes son revisadas y aprobadas por el personal autorizado. Una vez que el tiempo solicitado haya finalizado, el acceso es revocado.

X. REGISTRO DE INGRESO AL CENTRO DE CÓMPUTO

El acceso físico al centro de datos del proveedor de la nube es registrado y monitoreado con el fin de mejorar la seguridad según sea necesario.

Cuando se trate de visitantes, es necesario que presenten su identificación al llegar al sitio, firmar el registro de entrada e ir acompañados del personal autorizado.

XI. DISPOSITIVOS UTILIZADOS PARA EL ACCESO AL CENTRO DE CÓMPUTO

El acceso se encuentra controlado mediante videovigilancia, sistemas de detección de intrusiones y otros recursos electrónicos. El personal autorizado utiliza mecanismos de autenticación multifactor para tener acceso al centro de datos.

Los puntos de acceso físico a las salas de servidores utilizan cámaras de televisión de circuito cerrado (CCTV) para las respectivas grabaciones. Las imágenes se conservan de acuerdo con los requisitos legales y de conformidad.

XII. RESPALDO DE INFORMACIÓN DE LA AC

12.1. Esquema del sistema de respaldos

DICERT garantiza que toda la información relacionada con los certificados es almacenada por un período de tiempo apropiado. Todos los eventos que tengan lugar durante el ciclo de vida de un certificado digital son almacenados, incluyendo la renovación o revocación de éste.

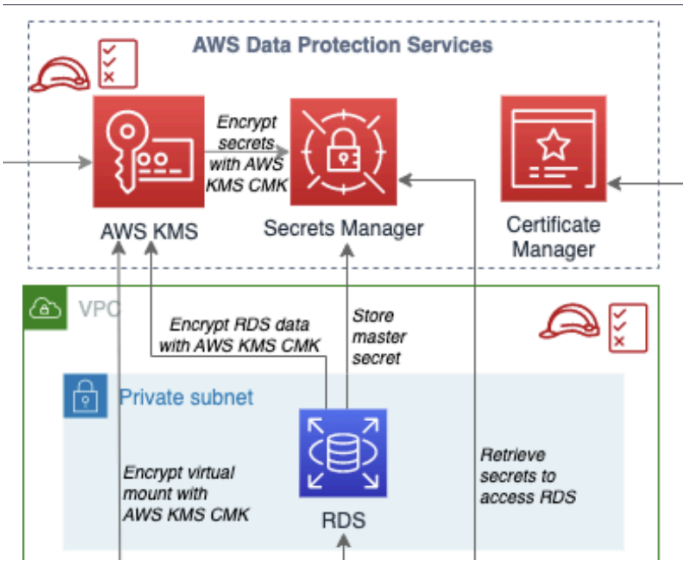

Figura 1. Diagrama de registros de control y trazabilidad (Fuente Amazon)

El sistema de recopilación de conservación se basa en la documentación entregada por los solicitantes para respaldar una solicitud de certificado. La documentación está almacenada en la base de datos del sistema para conservar dichos registros de acuerdo con las prácticas de retención y protección.

Todos los respaldos se almacenan cifrados, usando HSM conforme a FIPS 140-2 Nivel 3, y sólo personal autorizado puede acceder a estas copias.

12.2. Frecuencia y periodicidad de las copias de respaldo

El periodo de conservación depende del tipo de información y del nivel de confidencialidad de la información.

Se recomienda realizar una copia de respaldo mensualmente como medida de seguridad. Adicionalmente, toda la documentación relacionada con las solicitudes de certificados, así como los certificados emitidos se conservan por un período de 10 años.

12.3. Rotación de respaldos

La rotación de respaldos es responsabilidad de los administradores de DICERT. Todos los respaldos se etiquetan acorde con el tipo de información que contienen.

12.4. Ubicación física de los cartuchos de respaldos

El proveedor de la nube proporciona una consola centralizada de copias de seguridad para realizar el manejo de respaldos de una manera uniforme y de acuerdo con los requisitos de conformidad. Además, facilita las tareas de auditoría de los registros de actividad de respaldos y la garantía del cumplimiento normativo.

12.5. Respaldos de información

Se precisa almacenar ciertos datos personales de los solicitantes que son exclusivamente necesarios para la emisión de un certificado. Por lo cual se ha desarrollado una política que proteja dicha información.

Como parte de los respaldos de información se incluye:

- Documentos proporcionados para la solicitud de un certificado.
- Solicitudes de certificados, aprobadas o denegadas.
- Información personal obtenida para la emisión de un certificado.
- Registros de auditoría interna o externa.

12.6. Traslado registro y control de respaldos de llaves privadas

La custodia de las llaves privadas es otorgada a los propios titulares de los certificados, por lo que cualquier vulneración de la misma es entera responsabilidad del titular.

No obstante, con la única finalidad de llevar a cabo el proceso de firma electrónica de documentos, la llave privada se guarda también en los repositorios de la plataforma de firmas electrónicas. Para esto, la llave privada se almacena en un almacén de llaves (archivo de extensión p12), el cual se mantiene en una base de datos aislada en una subred privada (sin acceso a través de Internet) y se respalda en tiempo real hacia una base de datos de replicación.

Se recomienda a los titulares de los certificados utilizar una contraseña segura pero que al mismo tiempo sea fácil de recordar para evitar su pérdida, y por consiguiente la invalidez de la llave privada.

XIII. CONTROL DE CAMBIOS Y DOCUMENTACIÓN

Cada modificación al sistema será documentada incluyendo: versión de la actualización, fecha de aprobación, identificación del cambio, estado de la política, y ubicación de la política revisada. La información detallada sobre cada cambio es revisada y aprobada por el representante legal o su delegado, asegurando transparencia y continuidad.

Elaborado por:	**Firma**
Nombre: Sebastián Poveda Cargo: Encargado Seguridad de la Información	Firmado Digitalmente por: Sebastián Poveda Fecha2026-03-02T11:59:39-05:00 UUID:b709e906-706c-4936-b04

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