ArgosData - Signare

08 de agosto de 2022

Documento de Prácticas de Certificación

.

Documento de Prácticas de Certificación

Documento de Prácticas de Certificación

CONTROL DE VERSIONES

FECHA	AUTOR	VERSION	DESCRIPCION	FIRMA
22 de Junio 2022	Montran	0.01	Versión aprobada	
18 de agosto de 2022	Andrés Banda	1.00	Cambio a formato ArgosData	
16 de septiembre 2022	Montran	1.01	Actualización/Revisión de contenido	
19 de septiembre de 2022	Andrés Banda	1.02	Actualización a formato ArgosData	

Tabla de contenidos

1. Datos de Identificación de la Entidad de Certificación de Información y Servicios Relacionados Acreditada. 6

2. Objetivo 7

3. Introducción 8

4. Diagrama esquemático y descripción técnica detallada de la infraestructura 11

4.1. Detalle técnico de la infraestructura de llave pública 11

4.2. Jerarquía Entidad de Certificación de Información 13

4.3. Administración de la Autoridad de Certificación 14

4.3.1. Controles de procedimientos 14

4.3.2. Roles responsables del control y gestión de la infraestructura de llave pública 14

4.3.3. Identificación y autenticación para cada usuario autorizado 15

4.3.4. Roles que requieren segregación de funciones 15

4.3.5. Controles de personal 15

4.4. Roles y responsabilidades para generación y migración de llaves privadas 16

4.5. Procesos de auditoría de seguridad 16

4.5.1. Tipos de eventos generados 16

4.5.2. Frecuencia de procesado de registros de auditoría 17

4.5.3. Periodo de conservación de los registros de auditoría 17

4.5.4. Protección de los registros de auditoría 17

4.5.5. Procedimientos de respaldo de los registros de auditoría 17

4.5.6. Análisis de vulnerabilidades 17

5. Portafolio de servicios/productos de la entidad de certificación de información 19

5.1. Misión 19

5.2. Equipo humano 19

5.1. Detalle de productos y servicios de AC 19

5.2. Costos y tarifas de los servicios de certificación de información y servicios relacionados con la firma electrónica. 20

6. Políticas y condiciones de manejo de los Certificados de firma electrónica y de servicios relacionados. 21

6.1. Descripción y alcance detallado de cada servicio propuesto y de los recursos e infraestructura disponibles para su prestación 21

6.2. Descripción detallada del servicio propuesto como entidad de certificación 22

6.3. Mecanismos de validación: CRL, OCSP, LDAP 22
6.3.1. Servicio de listas de certificados revocados (CRL) 22
6.3.2. Servicio consulta en línea de certificados digitales (OCSP) 22
6.3.3. Servicio repositorio de certificados digitales (LDAP) 23
6.3.4. Sellado de tiempo (TSA – Time Stamp Authority) 23
6.3.5. Clientes potenciales 23
6.3.6. Condiciones del servicio 24
6.4. Servicios de emisión, renovación y revocación de certificados digitales 25
6.4.1. Obtención del certificado digital de persona natural 25
6.4.2. Obtención del certificado de un representante legal 26
6.4.3. Como resultado del proceso, el certificado digital y sus llaves asociadas son enviadas al titular mediante correo electrónico.Emisión del certificado digital 27
6.4.4. El certificado es generado en el formato estándar X.509 y es almacenado en la base de datos de la plataforma de firmas electrónicas para futuras consultas.Entrega certificado digital 28
6.4.5. Revocación del certificado 28
6.4.6. Renovación del certificado 30
6.4.7. Validez del certificado de firma electrónica de persona natural y representante legal 31
6.4.8. Aceptación de certificados 31
6.4.9. Firma y entrega del contrato 31
6.5. Autoridades de registro (AR) 32
6.5.1. Autoridad de registro 32
6.5.2. Autoridad de registro tercero vinculado 32
7. Condiciones de manejo de la información proporcionada por los usuarios 33
8. Límites de responsabilidad en la prestación de servicios de certificación de información y servicios relacionados con la firma electrónica. 36
9. Obligaciones de la entidad de certificación acreditada en la prestación de sus servicios. 37
10. Obligaciones de los usuarios y precauciones que deben observar en el manejo, uso y custodia de certificados y claves. 38
11. Garantías en el cumplimiento de las obligaciones que se deriven de las actividades de la entidad de certificación 39
12. Diagrama técnico detallado de cada "nodo" o "sitio seguro" y especificaciones técnicas de los equipos 40
12.1. Sitio seguro principal 40

12.1.1. Descripción del esquema de red 40
12.1.2. Dispositivos de seguridad de borde 41
12.1.3. Acceso a servicios desde internet 42
12.1.4. Conectividad LAN 42
12.1.5. Servidores 43
12.1.6. Almacenamiento 43
12.1.7. Sistema de respaldos 44
12.1.8. Red SAN 44
12.1.9. Data Center 44
12.1.10. Seguridad 44
12.1.11. Detalle de hardware y software 45
12.1.12. Ubicación y distribución de equipos en racks 46
12.1.13. Esquema de conectividad 46
12.1.14. Topología de conectividad 47
12.1.15. Esquema de cómputo 47
12.1.16. Hardware criptográfico HSM 49
12.1.17. Esquema de respaldos 50
12.2. Sitio seguro 50
12.2.1. Descripción del esquema de red 50
12.2.2. Almacenamiento 50
12.2.3. Red de comunicaciones 50
13. Ubicación geográfica de cada nodo o sitio seguro 51
13.1. Sitio principal 51
13.2. Sitio alterno 51
14. Documentos de soporte que confirmen que se dispone de mecanismos de seguridad 52
14.1. Mecanismos de seguridad 52
14.1.1. Seguridad a través de la criptografía 52
14.1.2. Certificado digital 52
14.1.3. Entidad de certificación 52
14.1.4. Algoritmo RSA 53
14.1.5. Algoritmo SHA 53
14.2. Contenedores criptográficos 53

14.3. Estándares y normas internacionales 53
14.3.1. Norma ISO/IEC 9594-8 estándar x.509 53
14.3.2. RFC 2560 – x.509 infraestructura de llave pública internet. PKI protocolo en línea del estado del certificado – OCSP (Online certificate status protocol) 54
14.4. Componentes de seguridad perimetral 55
14.4.1. Sistema de prevención de intrusos IPS 55
14.4.2. Firewall 56
14.4.3. Balanceadores 57
14.5. Esquema de seguridad perimetral 57
14.6. Esquema de seguridad de la infraestructura de llave pública – PKI 57
14.7. Plan de contingencia 57
14.8. Sistema de control de acceso al centro de cómputo 58
14.9. Registro ingreso centro de cómputo 58
14.10. Dispositivos utilizados para el acceso al centro de cómputo 59
14.11. Respaldo de información de la AC 59
14.11.1. Esquema del sistema de respaldos 59
14.11.2. Frecuencia y periodicidad de las copias de respaldo 60
14.11.3. Rotación de respaldos 60
14.11.4. Ubicación física de los cartuchos de respaldos 60
14.11.5. Respaldos de información 60
14.11.6. Traslado registro y control de respaldos de llaves privadas 60

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

Mediante Resolución ARCOTEL-2021-1060 del 28 de septiembre de 2021, la Agencia de Regulación y Control de las Telecomunicaciones emitió el Título Habilitante: Acreditación como una Entidad de Certificación de Información y Servicios Relacionados (ECI), mediante el cual otorga la Acreditación como Entidad de Certificación de Información y Servicios Relacionados a favor de la compañía ARGOSDATA CERTIFICACION DE INFORMACION Y SERVICIOS RELACIONADOS S.A.S. una empresa constituida bajo las leyes de la República del Ecuador con domicilio en la ciudad de Quito, identificada en redes con su nombre comercial ArgosData.

2. Objetivo

ArgosData es una compañía constituida con el fin de cubrir las necesidades del mercado ecuatoriano de firma electrónica y certificados digitales. Los servicios de certificación ofrecidos por ArgosData tienen como objetivo acreditar la identidad digital de las personas tanto naturales como representantes legales.

El objetivo de este documento de Prácticas de Certificación es de describir las condiciones, políticas y procedimientos aplicables a la solicitud, emisión, uso, suspensión y revocación de los certificados de firma electrónica, así como para la prestación de servicios relacionados, y las buenas prácticas utilizadas para la provisión de servicios de ArgosData para el ciclo de vida de certificados digitales.

ArgosData se compromete a cumplir en relación con la gestión de los certificados digitales las condiciones aplicables a la solicitud, expedición, uso y extinción de la vigencia de los certificados.

3. Introducción

El documento de Prácticas de Certificación establece las condiciones, políticas, principios y procedimientos aplicables a la solicitud, emisión, uso, suspensión y revocación, validación y administración de los certificados de firma electrónica, así como para la prestación de servicios relacionados y las buenas prácticas utilizadas.

Este documento de Certificación está estructurado según los lineamientos de la normativa ecuatoriana y del RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

Los principios y procedimientos que se detallan en este documento son:

- Ciclo de vida de un certificado y los controles operacionales.
- Detalles de los sistemas y operaciones de confianza.
- Aspectos técnicos sobre los certificados.
- Gestión de auditoría.
- Roles y responsabilidades de las partes involucradas dentro de la PKI de ArgosData.

Definiciones

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

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

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

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

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

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

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

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

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

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

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

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

Entidad de confianza: Es la entidad que confía en la información contenida en el certificado.

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

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

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

Acrónimos

Los acrónimos y abreviaciones que se usan a lo largo de este documento se definen en la siguiente tabla.

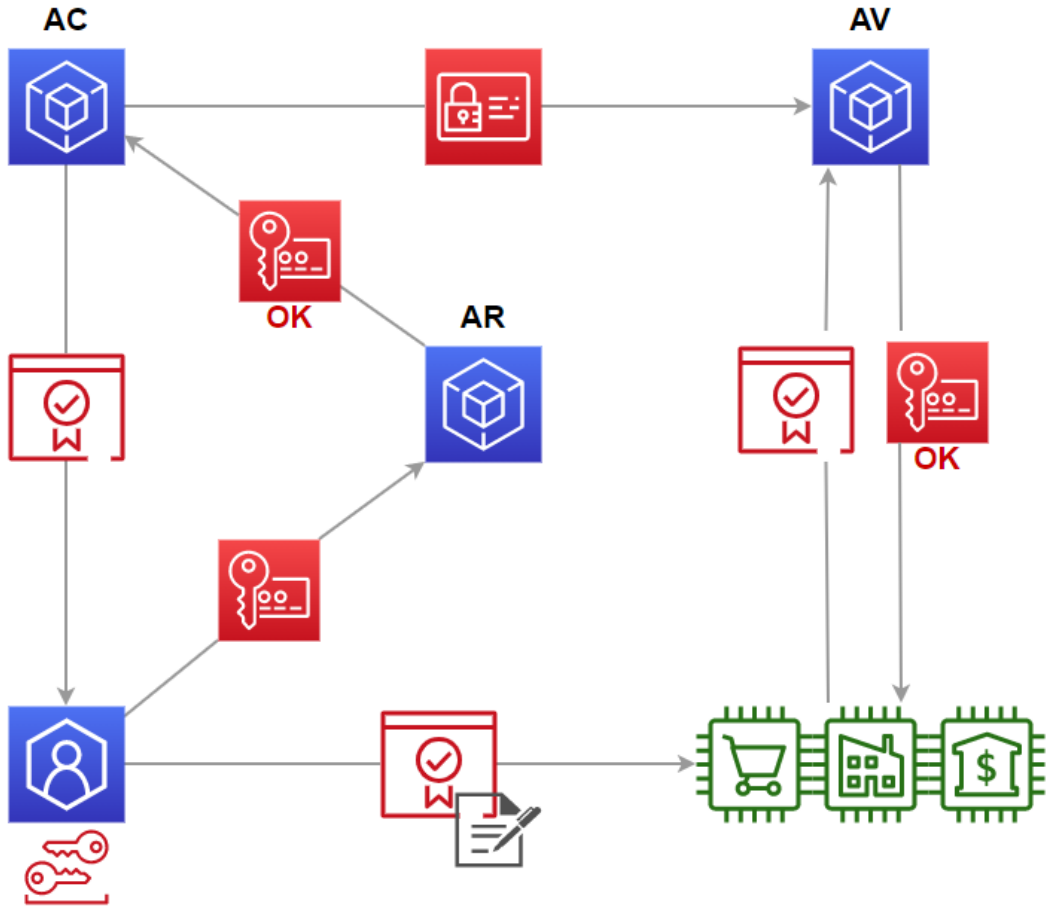
ACRÓNIMO	NOMBRE COMPLETO
AC	Autoridad de Certificación
AR	Autoridad de Registro
AV	Autoridad de Validación
CRL	Certificate Revocation List (Lista de Revocación de Certificados)
CN	Common Name (Nombre Común). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500
CSR	Certificate Signing Request (Solicitud de Firma de Certificado). Conjunto de datos que contienen una llave pública y su firma electrónica utilizando la llave privada

	asociada. Es enviada a la Autoridad de Certificación para la emisión de un certificado digital que contenga dicha llave pública.
DN	Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de la estructura de directorio X.500.
HSM	Hardware Security Module. Módulo de seguridad criptográfico utilizado para almacenar llaves y realizar operaciones criptográficas de modo seguro.
IEFT	Internet Engineering Task Force (Organismo de estandarización de Internet)
O	Organización. Atributo del DN dentro de la estructura de directorio X.500.
OSCP	Online Certificate Status Protocol. Este protocolo permite comprobar en línea la vigencia de un certificado digital.
OID	Object Identifier (Identificador de objeto único)
OU	Organizational Unit. Atributo del DN dentro de la estructura de directorio X.500.
PC	Política de Certificación
PKI	Public Key Infrastructure (Infraestructura de Llave Pública)
RFC	Request For Comments. Estándar emitido por la IEFT
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
TLS	Transport Layer Security
TSA	Time Stamping Authority
URL	Uniform Resource Locator

4. Diagrama esquemático y descripción técnica detallada de la infraestructura

4.1. Detalle técnico de la infraestructura de llave pública

Para la infraestructura de llave pública (PKI), ArgosData establece los siguientes componentes que se describen a continuación:



Acrónimos:

- AC: Autoridad de Certificación
- AR: Autoridad de Registro
- AV: Autoridad de Validación

Autoridad de Certificación Raíz

La Autoridad de Certificación Raíz (AC Raíz) basa su operatividad en un certificado emitido y firmado por sí misma. La AC Raíz solamente puede emitir certificados firmados por sí misma para Autoridades de Certificación Subordinadas.

El certificado de la AC Raíz no contiene la extensión certificatePolicies en su estructura por lo que no hay limitaciones en el conjunto de políticas de certificación que la AC Raíz puede cumplir.

Autoridad de Certificación Intermedia

La Autoridad de Certificación Intermedia (AC Intermedia) obtiene su certificado mediante el envío de una solicitud a la AC Raíz para emisión de un certificado de llave pública.

La AC Intermedia es una entidad subordinada a la AC Raíz y su función es emitir certificados para suscriptores dentro de su jurisdicción.

Autoridad de Registro

La Autoridad de Registro (AR) es el punto intermedio entre los solicitantes de un certificado digital y la Autoridad de Certificación.

Una de sus principales funciones es la de verificar las peticiones que hagan los solicitantes para obtener un certificado digital, comprobando la veracidad de los datos que se incluyen en las solicitudes, para que finalmente las envía a la Autoridad de Certificación para que sean procesadas.

Autoridad de Validación

La Autoridad de Validación (AV) ofrece 3 servicios para validación de un certificado:

- Validación en tiempo real mediante el protocolo OCSP.
- Validación mediante CRLs.
- Validación a través de una consulta directa del certificado en el portal de ArgosData.

Titular

El Titular hace referencia a una entidad o usuario final cuyo nombre es parte del campo Subject de un certificado.

Los siguientes tipos de titulares son admitidos en la PKI de ArgosData:

- Persona natural
- Representante legal

Entidades de confianza

Las entidades de confianza utilizan los certificados del Titular para validar la firma electrónica o sello de tiempo aplicados a un documento.

Para verificar la validez de un certificado digital, la entidad de confianza debe consultar la CRL publicada por la Autoridad de Validación. Adicionalmente la PKI de ArgosData facilita la validación mediante OCSP (Online Certificate Status Protocol).

Otros participantes

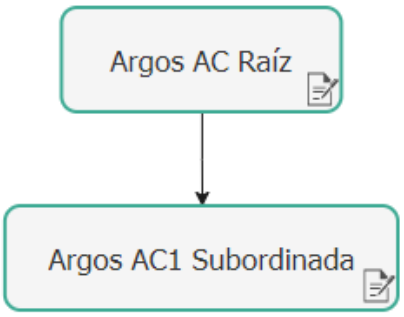
Solicitantes, son las personas físicas que solicitan la emisión de un certificado a la PKI de ArgosData.

Administradores de la AC, son las personas encargadas de gestionar y monitorear la infraestructura de la PKI.

4.2. Jerarquía Entidad de Certificación de Información

La jerarquía de certificación de información tiene como objetivo controlar la seguridad adecuada para cada división de tareas de las ACs que intervienen.

Para la prestación de los servicios ArgosData establece una jerarquía de entidad de certificación de dos niveles que permite políticas de administración, control y seguridad.



ArgosData AC Raíz

Es la entidad de certificación raíz definida en la jerarquía que tiene como propósito emitir certificados a otras entidades de certificación. Su certificado de llave pública es auto firmado.

ArgosData AC1 Subordinada

Es la entidad de certificación raíz definida en la jerarquía que tiene como objetivo emitir certificados a entidades finales. Su certificado de llave pública es firmado por ArgosData AC Raíz.

4.3. Administración de la Autoridad de Certificación

En esta sección se establecen los mecanismos de control de gestión y de operaciones en el dominio de creación de certificados de acuerdo con las políticas de certificación basados en el presente documento.

4.3.1. Controles de procedimientos

ArgosData garantiza que sus sistemas son operados de forma segura, por esta razón ha establecido procedimientos para las funciones que afectan a la provisión de sus servicios.

Para determinar la sensibilidad de la función para cada persona, se considera los siguientes puntos:

- Nivel de acceso.
- Habilidades requeridas.
- Deberes asociados a la función.

Se recomienda que existan 2 administradores de la AC y 2 administradores del sistema.

4.3.2. Roles responsables del control y gestión de la infraestructura de llave pública

Los roles son asignados por el equipo encargado de mantener y cumplir las operaciones relacionadas al procesamiento de los certificados, además de configuraciones adicionales para el correcto funcionamiento del ecosistema necesario para los certificados.

Son considerados como roles fiables:

- Administradores de la AC: encargados de la configuración del software de AC, incluyendo la generación de llaves de la AC, así como respaldo y recuperación de las mismas. Los administradores de la AC no emiten certificados a los solicitantes.
- Administradores del sistema: responsables de las configuraciones de acceso para individuos como Autoridades de Registro. Además, son los encargados de mantener las configuraciones del sistema propias para el manejo del ecosistema de certificados.
- Operadores de validación de solicitudes de certificados: conocidos como Autoridad de Registro, tienen a su cargo realizar la validación pertinente de las solicitudes de certificados para continuar con el proceso de emisión de éste.
- Operadores de revocación de certificados: comprometidos con la operación de revocación, cumpliendo oportunamente con las causas relacionadas para su procesamiento.

- Auditores internos: responsables de revisar, mantener, archivar logs de auditoría y llevar a cabo o supervisar el cumplimiento interno de la auditoría. Esto con el fin de determinar si ArgosData o la AR están operando.

Para los usuarios que pretendan gestionar sus certificados usando el portal web público de ArgosData, obtendrán un único rol como usuarios públicos del sistema.

4.3.3. Identificación y autenticación para cada usuario autorizado

El administrador del sistema es el responsable de identificar a cada usuario con su rol específico, con el fin de que puedan autenticarse posteriormente y tener acceso a sus funciones asignadas.

En el caso de la autenticación para el portal web público de ArgosData, se requiere del email del usuario, su contraseña, además de un código de seguridad que será enviado por correo electrónico para permitir continuar el proceso de solicitud de certificados.

En el caso de la autenticación para el portal web de administración de ArgosData, se requiere del email del usuario, su contraseña y el OTP (One time password) que es un valor numérico aleatorio generado criptográficamente por una aplicación móvil como Google Authenticator, para permitir el acceso a tareas de gestión de certificados.

4.3.4. Roles que requieren segregación de funciones

Los usuarios que hagan uso del portal web público de ArgosData, no podrán obtener otro rol que no sea el de usuario público.

Los usuarios que hagan uso del portal web de administración de ArgosData, podrán obtener más de un rol de acuerdo con sus funciones previamente acordadas.

4.3.5. Controles de personal

Es necesario emplear personal cualificado y con la experiencia apropiada para la prestación de servicios que ArgosData ofrece, tanto para los procedimientos de seguridad como para la gestión correcta. Por lo que se considera necesario que:

- Las personas que cuenten con roles fiables deben encontrarse libres de intereses personales que entren en conflicto con el desarrollo de la función a su cargo.
- Los administradores del sistema no podrán asignar un rol fiable o de gestión a una persona que no sea idóneo para el puesto.
- Se rechaza completamente que una persona que haya sido condenada por delito cuente con permisos o un rol para un puesto de gestión.

Para alcanzar una cualificación adecuada para la gestión de los servicios prestados por ArgosData, se deberá formar al personal incluyendo los siguientes contenidos:

- Mecanismos de seguridad referentes al ciclo de vida de un certificado.
- Tareas pertinentes al rol asignado para cada persona.
- Gestión y tramitación de incidentes.
- Procedimientos de gestión y de seguridad relacionadas con los datos de carácter personal de cada solicitante o titular de un certificado.

Cualquier personal que con conocimiento o negligencia viole las políticas de seguridad, abuse de su autoridad, o permita que personal bajo su supervisión viole las políticas de seguridad, puede ser sujeto de acciones disciplinarias que incluso podría terminar en la terminación de su contrato laboral.

Si las acciones realizadas por cualquier personal muestran una falla o deficiencia de capacitación entonces se recomienda llevar a cabo recapacitación para rectificar la acción.

4.4. Roles y responsabilidades para generación y migración de llaves privadas

Los roles que competen a las llaves privadas están netamente relacionados tanto con el solicitante de un certificado digital, así como con el software propiamente.

El solicitante tiene la responsabilidad de proveer una contraseña segura para el almacén de llaves que alojará el par de llaves. Así mismo, es responsabilidad del solicitante el utilizar una contraseña que sea fácil de recordar y mantenerla de manera segura. No se permite el cambio de contraseña de un almacén de llaves por lo que la pérdida de la contraseña implica revocar el certificado digital involucrado y solicitar un nuevo certificado digital.

El software de la plataforma de firmas electrónicas almacena la contraseña del almacén de llaves para propósitos de firma electrónica de documentos, por tanto es responsabilidad del software el almacenamiento seguro de la contraseña utilizando métodos de encriptación y asegurando que tanto el almacén de llaves como su contraseña se mantengan en un sitio sin acceso público.

4.5. Procesos de auditoría de seguridad

Para propósitos de auditoría, la aplicación guarda registros relacionados a los eventos y acciones que se llevan a cabo en la plataforma de firmas electrónicas.

4.5.1. Tipos de eventos generados

Se almacenan registros relacionados a eventos tales como:

- Inicio y finalización de ejecución del sistema.
- Intentos de crear, modificar o remover información de usuarios dentro del sistema.
- Intentos de autenticación de los usuarios en el sistema.
- Eventos que concierne al ciclo de vida de un certificado: solicitud, emisión, renovación y revocación.
- Intentos de modificación o remoción de parámetros del sistema utilizados para la gestión de los certificados.
- Intentos de ejecución de tareas programadas utilizadas para completar el ciclo de vida de un certificado.

4.5.2. Frecuencia de procesado de registros de auditoría

El procesamiento de los registros de auditoría consiste en una revisión que incluye la verificación de que los registros no hayan sido manipulados, además de una inspección de las entradas de registro que se hayan generado durante el procesamiento realizado por el sistema.

Es recomendable que los registros de auditoría sean examinados por lo menos una vez a la semana en busca de alguna actividad no habitual.

4.5.3. Periodo de conservación de los registros de auditoría

Los registros de auditoría deben ser conservados por al menos 10 años; tiempo fijado por la ley para la prescripción de acciones por daños y dentro del cual los registros pueden ser útiles o requeridos.

4.5.4. Protección de los registros de auditoría

Los registros de auditoría pueden ser accedidos sólo por un administrador del sistema. Además, los archivos de registros deben protegerse de lecturas, modificaciones, remociones o cualquier otro tipo de manipulación no autorizada.

4.5.5. Procedimientos de respaldo de los registros de auditoría

Se debe generar al menos una copia de respaldo de los registros mensualmente.

4.5.6. Análisis de vulnerabilidades

ArgosData intenta mitigar los riesgos a la plataforma de PKI mediante evaluaciones regulares de las amenazas y las vulnerabilidades del servicio, especialmente considerando la probabilidad de ocurrencia.

Se manejan diferentes categorías de evaluaciones: técnica, lógica, humana, ambiente y operacional.

5. Portafolio de servicios/productos de la entidad de certificación de información

5.1. Misión

Ser una compañía que brinde servicios de emisión de firmas electrónicas, sellado de tiempo y en general soluciones tecnológicas acordes con las necesidades legales modernas, como son el perfeccionamiento de actos y contratos a través de software y hardware altamente especializado.

5.2. Equipo humano

A desarrollarse según las necesidades internas, requerimientos del mercado y del proveedor de la infraestructura de PKI.

En términos generales consta de varias áreas:

1. Técnica
2. Administrativa
3. Comercial
4. Legal
5. Financiera y contable
6. Alta Gerencia
7. Junta General de socios y accionistas

5.1. Detalle de productos y servicios de AC

ArgosData brinda los servicios de Entidad Certificadora tales como la emisión, revocación y renovación de certificados digitales, poniendo a disposición del público el portal web público de ArgosData para la atención exclusiva de dichos servicios.

5.2. Costos y tarifas de los servicios de certificación de información y servicios relacionados con la firma electrónica.

Los costos y tarifas de los servicios que se brinden se mantendrán publicados en la página web de la entidad de certificación para conocimiento de sus usuarios y del público en general.

Hay servicios que no tienen costo como son:

a) El acceso a los certificados digitales emitidos bajo esta Política es gratuito, por lo que no se aplica ninguna tarifa.

b) El acceso a la información de estado o revocación es gratuito, por lo que no se aplica ninguna tarifa.

c) El uso del portal web para firma electrónica de documentos no tiene costo.

6. Políticas y condiciones de manejo de los Certificados de firma electrónica y de servicios relacionados.

6.1. Descripción y alcance detallado de cada servicio propuesto y de los recursos e infraestructura disponibles para su prestación

ArgosData emplea sistemas confiables que están protegidos contra toda alteración y que garantizan la seguridad técnica de los procesos de certificación a los que sirve de soporte.

Los servicios que se ponen a disposición son los siguientes:

- Validación de identidad de una persona mediante el uso de los servicios del Registro Civil Nacional.
- Emisión de un certificado por medio de una solicitud en línea.
- Renovación de un certificado por medio de una solicitud en línea
- Revocación de un certificado por medio de una solicitud en línea.
- Entrega de certificado de firma electrónica en archivo p12.
- Habilitación de firma electrónica.
- Publicación de CRLs.
- Validación del estado de un certificado por medio del servicio de consulta en línea de certificados digitales (OCSP).
- Descarga del certificado por medio del uso del portal web público de ArgosData.
- Descarga del archivo de almacén de llaves por medio del portal web público de ArgosData, siempre y cuando el usuario lo haya requerido.
- Firma o Solicitud de firma electrónica de documentos PDF.

Los servicios expuestos en línea se encuentran alojados en el proveedor de la nube, los mismos que se encuentran descritos posteriormente en este documento de Certificación.

6.2. Descripción detallada del servicio propuesto como entidad de certificación

Como entidad de certificación se prestan servicios tales como:

- Emisión de certificados digitales.
- Revocación de certificados digitales.
- Publicación de CRL.
- Publicación de Servicios OSCP para consulta de estado de certificado.

6.3. Mecanismos de validación: CRL, OCSP, LDAP

6.3.1. Servicio de listas de certificados revocados (CRL)

La verificación de las revocaciones es considerada obligatoria previo al uso de los certificados en los cuales los terceros desean confiar. Un método por el cual las entidades de confianza pueden verificar el estado de los certificados es consultando la CRL más reciente.

ArgosData publica CRLs para permitir que las entidades de confianza verifiquen una firma digital que ha sido generada usando un certificado digital emitido por ArgosData. Cada CRL contiene registros de todos los certificados revocados y no expirados que han sido emitidos y es válido por 24 horas.

ArgosData genera una nueva CRL cada 24 horas, la cual está identificada por un número secuencial autogenerado para cada CRL. Bajo circunstancias especiales, ArgosData publica una nueva CRL antes del tiempo de expiración de la CRL en curso.

Las CRLs se generan cada 7 días y se almacenan por un lapso de 10 años.

6.3.2. Servicio consulta en línea de certificados digitales (OCSP)

ArgosData expone un servicio para responder a solicitudes mediante el protocolo OCSP descrito en FRC 6960, el cual provee información en tiempo real acerca de la validez de un certificado. Este servicio facilita la consulta inmediata del estado de un certificado.

La respuesta a una petición del protocolo OCSP provee la siguiente información acerca del estado de un certificado:

- Good: El certificado es válido.
- Revoked: El certificado está revocado.

- Unknown: El certificado no fue emitido por la AC de ArgosData.

6.3.3. Servicio repositorio de certificados digitales (LDAP)

LDAP, al ser un protocolo ligero de acceso a directorio, es empleado como un mecanismo de gestión de los recursos del repositorio de certificados digitales en la AC Privada de AWS.

Cada comunicación LDAP incluye un cliente y un servidor con el fin de leer y escribir datos desde y hacia el repositorio de certificados, de esta manera se procura proteger los datos y cumplir con los requisitos de seguridad.

6.3.4. Sellado de tiempo (TSA – Time Stamp Authority)

ArgosData no ofrece el servicio de Sellado de tiempo, no obstante hace uso de una TSA externa para incluir un sello de tiempo como parte de la firma electrónica de documentos.

El servicio de sellado de tiempo permite incluir la fecha y hora dentro de los documentos firmados emitidos por un tercero de confianza. De esta forma se garantiza lo siguiente:

- El documento se firma y se crea en un instante de tiempo determinado.
- Los destinatarios de los documentos con un sellado de tiempo confiable pueden verificar que el documento no fue alterado después del envío.
- Se generan firmas seguras y legalmente admisibles.

El sellado de tiempo generado por la Autoridad de Sellado de Tiempo (TSA) cumple con el siguiente proceso:

- Al momento que una persona firma un documento, solicita el sellado de tiempo a la TSA.
- Se crea un hash y la TSA procede a combinar tanto el hash como el sellado de tiempo confiable.
- El resultado de la combinación es firmado digitalmente con la llave privada creando un token de sellado de tiempo.
- El token de sellado de tiempo es registrado en la firma del documento.

6.3.5. Clientes potenciales

El mercado de clientes demandando certificados de firma electrónica está en crecimiento, por ejemplo, para otorgamiento de actos notariales, comparecencia a asambleas de compañías y cooperativas, procedimientos contractuales en instituciones financieras, entre otros.

6.3.6. Condiciones del servicio

Las condiciones del servicio están determinadas por estas Prácticas de Certificación, los Términos y Condiciones de ArgosData, las Políticas de Seguridad y el Contrato con el usuario.

Obligaciones de la AC

Entre las obligaciones relevantes de la AC se consideran las siguientes:

- Proporcionar mecanismos de confianza para la generación de llaves y protección de éstas con respecto a su propia infraestructura.
- Proporcionar un aviso inmediato en caso de que se comprometa su llave privada.
- Emitir certificados digitales de acuerdo con este documento de Certificación.
- Actuar con rapidez para la emisión de un certificado al recibir una solicitud de una Autoridad de Registro.
- Actuar con inmediatez al recibir una solicitud de revocación por parte de una Autoridad de Registro.
- Publicar certificados de acuerdo con este documento de Certificación.
- Brindar soporte cuando lo requieran las partes que confían en los certificados.

Obligaciones de la AR

Entre las obligaciones relevantes de la AR se consideran las siguientes:

- Recibir solicitudes de certificados de acuerdo con lo establecido en este documento de Prácticas de Certificación.
- Realizar todas las acciones oportunas para la verificación de las solicitudes de certificado.
- Recibir las solicitudes de revocación de un certificado de acuerdo con lo establecido en este documento de Certificación.
- Actuar de acuerdo con las leyes y regulaciones pertinentes.

Obligaciones de los titulares de los certificados

El titular tiene como obligación aceptar los Términos y Condiciones relacionados al servicio solicitado. Al aceptarlos, el titular está de acuerdo con este documento de Certificación y la Política de Certificación respectivamente. En caso de no aceptar, no se le será proporcionado el servicio por ningún medio.

Obligaciones de los terceros aceptantes

Los terceros aceptantes tienen como obligación:

- Verificar minuciosamente cada firma electrónica de un certificado.
- Asegurarse que el certificado no pertenezca a la lista certificados revocados.
- Comprobar que el certificado pertenece a una Autoridad de Certificación debidamente autorizada por el organismo de control pertinente.
- Confiar sólo en aquellos certificados de llaves públicas que se utilizan de acuerdo con su finalidad y correspondiente a su área aplicable.

6.4. Servicios de emisión, renovación y revocación de certificados digitales

El propósito de esta sección es describir los requisitos operacionales que ArgosData ha establecido para el manejo del ciclo de vida de los certificados con respecto al registro, la identificación, la validación, emisión, renovación y revocación de éstos.

6.4.1. Obtención del certificado digital de persona natural

El proceso para que una persona natural solicite un certificado incluye los pasos descritos a continuación:

- El solicitante debe registrarse en el portal web público de ArgosData y posteriormente completar el proceso de autenticación.
- Una vez que el solicitante es registrado como usuario, debe llenar un formulario compuesto por datos personales y cargar documentos que justifiquen la información ingresada. Para una persona natural se solicita:

DATOS PERSONALES	DOCUMENTOS
- Tipo de persona - Número de Identificación - **Código dactilar** - Número de Identificación para Impuestos (RUC – si aplica) - Nombres - Apellidos - País - Estado/Provincia - Ciudad - Dirección de Domicilio - Número de Teléfono	- Cédula de Ciudadanía o Pasaporte - Video indicando la voluntad de solicitar un certificado electrónico.

- Este proceso está respaldado legalmente por la aceptación de los Términos y Condiciones al registrarse como usuario, una Declaración de Voluntad en video y un Contrato presentados como primer y último paso del formulario respectivamente.
- El solicitante tiene la responsabilidad de veracidad y de confirmar sus datos personales y asegurar que la documentación está completa para el registro de la solicitud de certificado.
- Como resultado del proceso, el certificado digital y sus llaves asociadas son enviadas al titular mediante correo electrónico.

6.4.2. Obtención del certificado de un representante legal

El proceso para que un representante legal solicite un certificado incluye los pasos descritos a continuación:

- El solicitante debe registrarse en el portal web público de ArgosData y posteriormente completar el proceso de autenticación.
- Una vez que el solicitante es registrado como usuario, debe llenar un formulario compuesto por datos personales y cargar documentos que justifiquen la información ingresada. Para una persona jurídica se solicita:

DATOS DE LA ENTIDAD	DOCUMENTOS
- **Tipo de persona** - **Número de identificación** - **Código dactilar** - **Nombres** - **Apellidos** - **País** - Estado/Provincia - Ciudad - Dirección de domicilio - Número de teléfono - Cargo en la empresa - Nombre de la empresa - Razón social de la empresa - Número de Identificación para Impuestos de Compañía (RUC) - **Registro único de proveedores (RUP)** ○	- Cédula de Ciudadanía o Pasaporte del Representante Legal - Escritura de Constitución de la empresa - Nombramiento del Representante Legal - Video indicando la voluntad de solicitar un certificado electrónico.

- Este proceso está respaldado legalmente por la aceptación de los Términos y Condiciones al registrarse como usuario, una Declaración de Voluntad en video y un Contrato presentados como primer y último paso del formulario respectivamente.
- El solicitante tiene la responsabilidad de veracidad y confirmar sus datos personales y asegurar que la documentación está completa para el registro de la solicitud de certificado.

6.4.3. Como resultado del proceso, el certificado digital y sus llaves asociadas son enviadas al titular mediante correo electrónico.Emisión del certificado digital

Durante el proceso de ingreso de datos, se verifica la identidad del solicitante, ArgosData hace uso de servicios del Registro Civil Nacional que contiene un amplio repositorio de la población del país. En caso de que la respuesta sea negativa, no se permite seguir con el proceso de solicitud.

Procesamiento de la solicitud de certificado

Una vez que la solicitud del certificado digital haya sido enviada, la Autoridad de Registro es la encargada de dar inicio al procesamiento de la misma realizando una verificación de los datos proporcionados.

Para verificar la identidad del solicitante, ArgosData hace uso de servicios de reconocimiento facial de AWS, que contiene varias métricas de verificación para encontrar la similitud entre el video y la foto recuperada del Registro Civil Nacional al momento de ingresar los datos. En caso de que la respuesta sea negativa, la persona es notificada por correo electrónico.

Cuando la documentación del solicitante es insuficiente o no concuerda con el resto de la información enviada, la Autoridad de Registro tiene la potestad de rechazar la solicitud de certificado. Inmediatamente la persona es notificada por correo electrónico con el motivo del rechazo.

En caso de que todos los datos presentados, la documentación y la información del Registro Civil y el reconocimiento facial estén correctos, la Autoridad de Registro aprueba la solicitud para que se continúe con su emisión.

ArgosData se reserva el derecho de rechazar una Solicitud de Certificado Digital a cualquier entidad según crea conveniente, sin incurrir en responsabilidades por alguna pérdida o gastos que se generen.

Procedimiento de emisión del certificado

ArgosData genera el certificado digital por medio del portal de administración de ArgosData, el mismo que valida que la Autoridad de Registro tiene los permisos necesarios para completar el proceso de autenticación y que esté autorizada para emitir el certificado. De esta manera se asegura que la comunicación entre la AR y la AC se realiza de forma segura y confiable.

Las acciones a realizarse para la emisión del certificado digital consisten en:

- Los datos de la solicitud de certificado ya aprobada están disponibles en el portal de administración de ArgosData.
- ArgosData genera un CSR (Certificate Singing Request) que es posteriormente enviado a la AC.
- Utilizando el CSR, la AC emite un certificado digital que está firmado con la llave privada de la AC Subordinada.

6.4.4. El certificado es generado en el formato estándar X.509 y es almacenado en la base de datos de la plataforma de firmas electrónicas para futuras consultas.Entrega certificado digital

Una vez que ha concluido la emisión del certificado digital, este junto con sus llaves asociadas son enviadas al titular mediante correo electrónico.

Adicionalmente, el portal web público de ArgosData pone a disposición del titular el acceso al almacén de llaves y el certificado digital para su descarga. Para este cometido, es necesario que la persona haya cumplido con el proceso de autenticación satisfactoriamente.

El solicitante tiene la obligación de verificar el contenido del certificado, es decir que la información está completa y correcta. Si el certificado tiene errores, el solicitante debe informar a la AC inmediatamente y solicitar la revocación.

6.4.5. Revocación del certificado

La revocación deja sin efecto la validez de un certificado antes de su caducidad. Es un proceso irreversible, es decir, una vez que un certificado sea revocado, éste ya no puede ser renovado por ninguna circunstancia.

Causas de revocación del certificado

Es permitido realizar la revocación de certificados bajo las siguientes causas:

- Causas que afectan la seguridad de la llave o del certificado:
    - La llave privada o la infraestructura utilizada para la emisión del certificado es comprometida y afecta la fiabilidad de los certificados emitidos a partir de un incidente.
    - Infracción, por parte de ArgosData, de los requerimientos definidos en los procedimientos de gestión de certificados establecidos en este documento de Certificación.
    - Acceso no autorizado o uso indebido por un tercero de la llave privada del titular.

- La falta de diligencia en la custodia de la llave privada por parte del titular.
- ArgosData es notificado de alguna circunstancia que indica que el nombre del dominio o el titular no están legalmente habilitados a utilizar el certificado ya sea por decisión de una corte o árbitro.

- Causas que afectan al titular o poseedor de llaves:
  - Infracción del titular en cuanto a sus obligaciones, responsabilidades y garantías establecidas en este documento de Certificación.
  - ArgosData considera razonablemente que ha existido pérdida, robo, modificación, divulgación no autorizada, o cualquier otra razón que comprometa la llave privada asociada con el certificado.
  - El fallecimiento del titular.
- Otras causas:
  - La culminación del servicio por parte de ArgosData.
  - El titular solicita por escrito que la AC revoque el certificado.
  - Un certificado fue emitido como resultado de fraude o negligencia.
  - Cuando el certificado compromete el estado de confianza de ArgosData.
  - Otras determinadas por la ley o los reglamentos.

Quién puede solicitar la revocación de un certificado

Están autorizados para solicitar la revocación de un certificado:

- La persona o titular a nombre del cual el certificado fue emitido.
- La Autoridad de Registro a nombre del titular del certificado.
- La Autoridad de Registro a su nombre, solamente si tiene la evidencia que justifica la revocación del certificado.
- Otras determinadas por la ley o los reglamentos.

Procedimiento de solicitud de revocación

Por medio del portal web público de ArgosData, la persona o titular del certificado puede iniciar con la solicitud de revocación. Una vez escogido el certificado válido y de haber ingresado la razón de revocación, el sistema se encargará de enviar un código de seguridad al correo electrónico del titular. Si el código ingresado es válido, la solicitud será enviada y procesada por la AC.

Por el otro lado, para que la Autoridad de Registro tramite una solicitud de revocación, realiza la búsqueda de un certificado por medio del documento de identidad o pasaporte del titular y envía

directamente la solicitud a la AC para su procesamiento respectivo, sin necesidad de ningún método de seguridad adicional.

Cuando este procedimiento sea completado, el certificado es añadido a la CRL y el sistema envía una notificación por correo electrónico a la persona o titular informando acerca de la revocación exitosa. Ni el titular ni la Autoridad de Registro podrán reactivar el certificado una vez revocado.

6.4.6. Renovación del certificado

Todas las renovaciones se realizarán con cambio de llaves, sin tomar en cuenta su causa.

Causas de renovación del certificado

Un certificado puede ser renovado por los siguientes motivos:

- El periodo de validez está por expirarse.
- Es necesario el cambio de datos contenidos en el certificado.
- Las llaves corren riesgo de vulnerabilidad.

Quién puede solicitar la renovación de un certificado

La solicitud de renovación es realizada por el titular para que se pueda realizar la emisión y entrega de un certificado renovado.

Procedimiento de solicitud de renovación

Por medio del portal web público de ArgosData, el titular inicia la solicitud de renovación a partir de un certificado aún vigente y se procede con lo siguiente:

- ArgosData utiliza la información de la solicitud de certificado original relacionada con el certificado seleccionado, excepto los archivos de documentos asociados. Esto con el fin de que la Autoridad de Registro pueda realizar la verificación pertinente con una documentación actualizada.
- El solicitante tiene la facultad de decidir si mantiene los mismos datos personales o de la empresa según sea el caso, o a su vez modificar la información.
- Una vez que el titular envíe la solicitud de renovación, se continúa con los mismos pasos establecidos en la sección 6.4.1 o 6.4.2 de este documento de Certificación., según corresponda.
- Finalmente, el certificado original es identificado como revocado, en consecuencia, ya no estará disponible para una nueva renovación.

6.4.7. Validez del certificado de firma electrónica de persona natural y representante legal

Los certificados y su par de llaves asociados tienen un periodo de uso de acuerdo con lo que el solicitante haya seleccionado durante la solicitud de certificado.

ArgosData ofrece certificados con diferentes períodos de validez y costos. Los periodos serán estipulados por ArgosData conforme la ley vigente y podrán ser modificados según se requiera. El período de validez de un certificado emitido por la AC de ArgosData es máximo de 3 años.

La culminación de la validez de un certificado se produce en los siguientes casos:

- Revocación del certificado por cualquiera de las causas estipuladas en la sección 6.4.5 de este documento de Certificación.
- Expiración de la vigencia del certificado.
- ArgosData cesa sus operaciones.

6.4.8. Aceptación de certificados

La aceptación del certificado por parte del solicitante inicia desde el momento que es notificado por su emisión válida. Con la aceptación del certificado el solicitante declara que:

- Toda la información entregada en el proceso de solicitud de certificado es verídica.
- El certificado será usado única y exclusivamente para fines legales y autorizados.
- El certificado será válido siempre y cuando no haya caducado y no haya sido revocado.

6.4.9. Firma y entrega del contrato

El contrato de prestación de servicios de certificación tiene como objetivo informar los derechos y obligaciones del usuario y de ArgosData. Igualmente, incluye las definiciones técnicas y legales básicas para que el titular tenga el conocimiento de las acciones a realizarse, así como de sus obligaciones ante ArgosData.

ArgosData hace la entrega del contrato a cada titular durante la generación de una solicitud de certificado por medio del portal público de ArgosData. Es obligatorio haber leído y aceptado el contrato para poder realizar el envío de la solicitud de certificado digital.

6.5. Autoridades de registro (AR)

6.5.1. Autoridad de registro

ArgosData ha implementado la infraestructura necesaria para gestionar el ciclo de vida de los certificados digitales dentro de la PKI. Para esto se ha establecido un grupo de Autoridades Registradoras (ARs) que ofrecen y hacen uso de los servicios de la CA cumpliendo con las siguientes funciones:

- Verificar la identidad de un suscriptor, analizando la información proporcionada en la Solicitud de Certificado y comparando con 2 fuentes adicionales de información:
    - Documentos que sustentan la información (notarizada para ciertos documentos)
    - Información obtenida a partir de los servicios que ofrece el Registro Civil del Ecuador.
- Aprobar o rechazar el registro de una Solicitud de Certificado.

Adicionalmente al procesamiento de las Solicitudes de Certificado Digital, la AR ejecuta:

- Verificación, aprobación y rechazo de Solicitudes de Renovación.
- Solicitud de Revocación de certificado.

6.5.2. Autoridad de registro tercero vinculado

Los servicios de certificación de información podrán ser proporcionados y administrados en todo o en parte por terceros. Para efectuar la prestación, éstos deberán demostrar su vinculación con la Entidad de Certificación de Información acreditada para el efecto, en este caso ArgosData. La autoridad competente establece los términos bajo los cuales las Entidades de Certificación de Información pueden prestar sus servicios por medio de terceros. (Art. 33 LCEFMD)

7. Condiciones de manejo de la información proporcionada por los usuarios

6.1 Almacenamiento de información. - Mientras el usuario haga uso de los servicios de ArgosData su información debe ser conservada. Si un usuario deja de utilizar los servicios de ArgosData, 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 ArgosDatale 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 ArgosDataconservará 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 ArgosData.

6.2. Información que se comparte y autorización del usuario para el efecto. - ArgosData entiende la naturaleza sensible de la información personal y en consecuencia la información que el usuario provee a ArgosData estará protegida y no será compartida con terceros no relacionados, en los términos establecidos por la ley.

A pesar de que ArgosData no comparte la información personal con terceros no relacionados, el usuario puede explícitamente indicar que su información no sea compartida en el futuro a través del envío de una solicitud al correo electrónico soporte@argosdata.com.ec. ArgosData 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 le informaremos de la misma. Si un usuario solicita la no compartición de su información durante el periodo de vigencia en que ArgosData le está prestando un servicio y la prestación del servicio depende de esa 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 ArgosData 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 ArgosData 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.

ArgosData 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 ArgosData , y utilizados por éstos, incluyendo, pero sin limitarse a proveedores, empresas asociadas o filiales de la Compañía.

6.3 Declaración del Usuario. - En el contrato a ser suscrito por el usuario, el usuario de manera expresa declarará que ha leído y comprendido las Políticas de Certificación de ArgosData, los Términos

y Condiciones de ArgosData y el contenido total del contrato, por lo que los acepta de manera voluntaria y presta su consentimiento expreso e inequívoco de regirse a los mismos.

8. Límites de responsabilidad en la prestación de servicios de certificación de información y servicios relacionados con la firma electrónica.

ArgosData no asume ninguna responsabilidad por firmas, certificados, o cualquier otro servicio o documento relacionado, que sean usados de manera incorrecta o para fines ilícitos, o para aquellos fines que excedan los límites de buen uso contemplados en el contrato, en el certificado, en los Términos y Condiciones de Uso o las Prácticas de Certificación.

ArgosData no será responsable en los siguientes casos:

1. Interrupciones o demoras en el servicio por causas de fuerza mayor o caso fortuito.
2. Interrupciones o demoras en el servicio por causas ajenas a ArgosData, o imputables a terceros como puede ser el prestador de servicio de conectividad vía internet o la conectividad con el Registro Civil para la validación de información, entre otros.
3. Responsabilidad por daños y perjuicios que ocasionare el titular del certificado de firma electrónica a terceros.

9. Obligaciones de la entidad de certificación acreditada en la prestación de sus servicios.

1. Actuar de acuerdo con las leyes y regulaciones pertinentes.
2. Actuar con rapidez para la emisión de un certificado.
3. Brindar soporte cuando lo requiera el usuario.
4. Guardar confidencialidad respecto de la información que obtenga por parte del usuario.
5. Actuar de forma inmediata para la suspensión o revocatoria de certificados cuando exista orden de autoridad competente.
6. Haber otorgado la garantía de responsabilidad conforme manda la ley y descrita en el presente contrato.

10. Obligaciones de los usuarios y precauciones que deben observar en el manejo, uso y custodia de certificados y claves.

1. Actuar de acuerdo con las leyes y regulaciones pertinentes.
2. Brindar información correcta, completa y veraz, de manera oportuna.
3. Acatar los Términos y Condiciones de ArgosData, aceptados por el usuario. Al aceptar los términos y condiciones, el titular está de acuerdo con la Política Privacidad y de Cookies. Así mismo de manera expresa manifiesta que ha leído, conoce y está de acuerdo con la Política de Prácticas de Certificación y Seguridad respectivamente.
4. Acatar las políticas de Practicas de Certificación y Seguridad de ArgosData, aceptadas por el usuario.
5. Cumplir con las obligaciones contractuales.
6. Utilizar de manera correcta la plataforma, los certificados y la firma, para fines lícitos.
7. Responder por el uso de la firma electrónica.
8. No exceder los límites de uso contemplados en el presente contrato, los Términos y Condiciones y la Política de Certificación.
9. Informar a ArgosData sobre cualquier cambio en la información utilizada para la obtención del certificado de firma electrónica.
10. El certificado de firma electrónica no podrá utilizarse para fines ilícitos o que contravengan las disposiciones legales de la República del Ecuador, especialmente pero no limitado al Código de Comercio, Código Civil, Código Integral Penal, a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su Reglamento.
11. El certificado de firma electrónica no podrá ser utilizado por un tercero distinto a su titular, ni aun cuando el tercero cuente con el consentimiento del titular, pues el certificado es de uso único y exclusivo de su titular, quedando expresamente prohibido el delegar el uso de este.
12. El certificado de firma electrónica no podrá utilizarse en contravención de cualquier disposición contemplada en el presente contrato, los Términos y Condiciones de ArgosData y su Política de Certificación.
13. Actuar con diligencia y cuidado en la custodia y manejo de su firma electrónica.

11. Garantías en el cumplimiento de las obligaciones que se deriven de las actividades de la entidad de certificación.

En concordancia con el artículo 30 literal h) de la Ley No, 67, ArgosData establece una garantía de responsabilidad con la finalidad de asegurar a los usuarios el pago de daños y perjuicios como resultado por el incumplimiento de sus obligaciones.

1. En el evento de incumplimiento de obligaciones ArgosData asumirá hasta un valor equivalente al 100% del precio pagado por el Usuario por la firma electrónica contratada.
2. Conforme lo establecido por el Reglamento a la Ley de Comercio Electrónico, para la ejecución de la garantía el procedimiento consistirá en que el usuario presente a la autoridad nacional competente (ARCOTEL al momento), una solicitud motivada en el término de 15 días a partir de que se produjo el supuesto incumplimiento, para que al amparo de lo dispuesto en el artículo 31 de la Ley No. 67, ésta ponga en conocimiento de ArgosData el reclamo formulado.
3. A partir de la comunicación recibida por ArgosData, la ECI tendrá 5 días término para presentar sus descargos, resolver dicho reclamo o reconocer el incumplimiento.
4. Una vez fenecido el término antes referido, dentro del término de 5 días posteriores la autoridad nacional competente deberá resolver sobre la procedencia del reclamo formulado, y de ser el caso ordenar la ejecución parcial de la garantía de responsabilidad por el monto de los daños y perjuicios causados y debidamente probados, los que no podrán reconocerse por un valor superior al pactado en el contrato y que son de un valor equivalente al 100% del precio pagado por el Usuario por la firma electrónica contratada. Sin perjuicio de lo anterior, el usuario podrá considerar el inicio de las acciones que estime pertinentes en contra de la Entidad de Certificación de Información y Servicios Relacionados, por los daños y perjuicios no cubiertos por la garantía de responsabilidad.
5. En cualquier caso, el usuario tiene la obligación de probar de manera adecuada y objetiva el daño sufrido, así como su relación de causalidad con el supuesto incumplimiento.

12. Diagrama técnico detallado de cada "nodo" o "sitio seguro" y especificaciones técnicas de los equipos

12.1. Sitio seguro principal

12.1.1. Descripción del esquema de red

La arquitectura de red ha sido diseñada sobre los servicios e infraestructura de AWS (Amazon Web Services). Los componentes de la arquitectura de red son:

DNS: El componente de DNS corresponde al servicio Route 53 de AWS, el cual permite el registro de los dominios utilizados para los portales web de acceso público y administración.

Balanceador de Carga: Basado en el servicio ELB (Elastic Load Balancing) para control del tráfico entrante y saliente hacia la Red Privada Virtual (VPC).

Región AWS: Ubicación que agrupa Zonas de Disponibilidad, las cuales están separadas físicamente y corresponden con Centros de Datos.

Zona de Disponibilidad: Ubicada dentro de una Región AWS, se trata de un Centro de Datos.

VPC: La Red Privada Virtual (por sus siglas en inglés) es un servicio de AWS para definir un grupo de subredes aisladas y con capacidad para conectarse a la red privada de una empresa.

Grupo de Seguridad: Conjunto de reglas de entrada y salida, actúa como firewall para controlar el tráfico entrante y saliente de la VPC.

Subredes: Las subredes son configuradas como públicas o privadas, una subred pública tiene acceso a Internet mientras la subred privada solamente tiene accesos a recursos dentro de la VPC.

Instancia EC2: Es una instancia de servidor virtual que cuenta con recursos asignados que no se comparten con otros servidores. La estrategia de recuperación ante desastres es Warm-standby, la cual permite mantener la instancia primaria ejecutándose con el 100% de recursos y se encarga de procesar todo el tráfico entrante, en tanto que la instancia secundaria se encuentra en standby con recursos limitados y se encuentra lista para tomar control del tráfico entrante cuando la instancia primaria falla.

Base de Datos: Desplegado sobre una instancia EC2, es el motor de base de datos que gestiona el almacenamiento de la información. La base de datos realiza replicación sincrónica propia de PostgreSQL con su equivalente en la Zona de Disponibilidad secundaria.

AC Privada: Servicio de AWS que permite emitir certificados, generar llaves, revocar certificados y publicar CRLs.

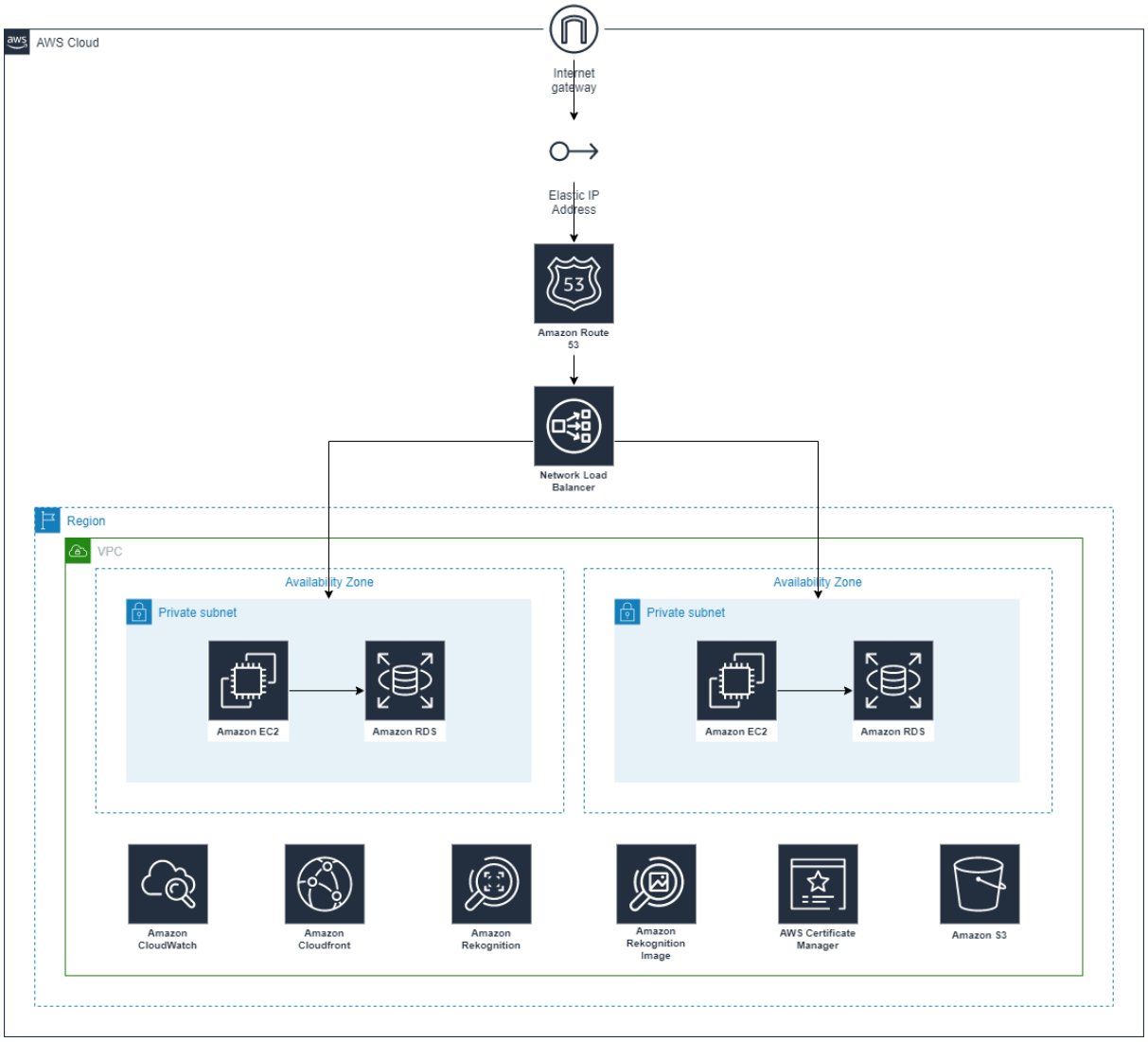


Gráfico 1. Arquitectura de Red

12.1.2. Dispositivos de seguridad de borde

La infraestructura de AWS utiliza dispositivos y sistemas para registrar y monitorear el acceso a los centros de datos y aplicaciones de AWS.

Cámaras

Las habitaciones de servidores están monitoreadas constantemente por un Circuito de Cámaras de Televisión Cerrado (CCTV).

Puntos de Entrada

Se utilizan sistemas de vigilancia, sistemas de detección, dispositivos de autenticación y dispositivos de alarma.

Fuente de Energía

Los centros de datos de AWS están equipados con fuentes de energía de respaldo para asegurar que la energía está disponible las 24 horas al día en caso de una falla eléctrica.

Clima y Temperatura

AWS cuenta con sistemas de control de la temperatura para asegurar que el hardware opere bajo las condiciones de temperatura adecuadas.

Detección de incendios y prevención

Se utilizan sensores de detección de humo en todos los espacios de la infraestructura. Así mismo existen sistemas de supresión para control de incendios.

Detección de fugas

Existen mecanismos para detectar la presencia de agua y así mismo existen mecanismos para remover el agua en caso de ser necesario.

https://aws.amazon.com/compliance/data-center/controls/

12.1.3. Acceso a servicios desde internet

El acceso a los sistemas y administración de los mismos se lleva a cabo a través de una VPC.

Una VPC (nube privada virtual) es una red virtual dentro de la nube de AWS. Dentro de la VPC se configuran diferentes subredes con el fin de aislar las diferentes capas de la aplicación.

Se utiliza una subred sin acceso a internet para alojar a la base datos.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/infrastructure-security.html

12.1.4. Conectividad LAN

La conectividad dentro de la VPC se establece y configura mediante una interfaz de red lógica, la cual representa a una tarjeta de red virtual.

La interfaz de red puede ser creada, acoplada a una instancia, desacoplada de la instancia y acoplada a una instancia diferente de tal forma que esta última reciba el tráfico de la anterior.

- Una interface de red incluye atributos como:
- Una dirección IPv4 privada primaria
- Una dirección IPv4 privada secundaria

- Una dirección IPv4 pública
- Una o más direcciones de IPv6 primarias
- Uno o más grupos de seguridad (reglas de control para tráfico de entrada y salida)
- Una dirección MAC
- Un parámetro para permitir verificación de fuente/destino

El ancho de banda que soporta una instancia de servidor EC2 es de hasta 5 Gb/s y con un MTU de 1500 bytes.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/network_mtu.html

12.1.5. Servidores

Las aplicaciones que componen la plataforma de PKI se instalan sobre instancias AWS EC2 de tipo T4g.

El almacenamiento es controlado mediante el servicio de AWS EBS, el cual permite crear volúmenes de almacenamiento y atarlos a instancias EC2. Los volúmenes creados son ubicados dentro una Zona de Disponibilidad específica donde son replicados automáticamente.

Los volúmenes de EBS permiten tomar capturas (snapshots) para respaldos y recuperación.

Para más información sobre las instancias de EC2 revisar la siguiente URL:

https://aws.amazon.com/ec2/instance-types/

12.1.6. Almacenamiento

El almacenamiento dedicado al repositorio de datos es gestionado por Amazon Relational Database Service (RDS) el cual automatiza procesos de aprovisionamiento de hardware, configuración de base de datos, software patching y respaldos.

El motor de base datos utilizado para gestionar el repositorio de datos es PostgreSQL.

El almacenamiento es controlado mediante el servicio de AWS EBS, el cual permite crear volúmenes de almacenamiento y atarlos a instancias EC2. Los volúmenes creados son ubicados dentro una Zona de Disponibilidad específica donde son replicados automáticamente.

Los volúmenes de EBS permiten tomar capturas (snapshots) para respaldos y recuperación.

Para más información acerca del servicio RDS Postgres revisar la siguiente URL:

https://aws.amazon.com/rds/postgresql/features/?nc=sn&loc=2&dn=1

12.1.7. Sistema de respaldos

Los respaldos son gestionados a través de Amazon EBS. El volumen asociado a una instancia EC2 se replica a través de múltiples servidores dentro de la Zona de Disponibilidad para prevenir la pérdida de datos si algún componente falla.

Los respaldos pueden ser configurados para que se lleven a cabo automáticamente a través de las opciones de configuración de Amazon EBS. Además, Amazon brinda la posibilidad de obtener snapshots del volumen de la instancia EC2, los cuales se utilizan principalmente para restaurar un volumen, entre otras opciones relacionadas con la gestión de volúmenes en Amazon EBS.

Igualmente, los respaldos de base de datos son gestionados por Amazon RDS de forma automática. Amazon RDS respalda la base de datos y los logs de transacciones, y los almacena por un período de retención de 35 días.

Adicionalmente, también el usuario puede iniciar respaldos mediante Snapshots de la instancia de base de datos. Los respaldos completos se almacenan en Amazon RDS hasta que sean borrados explícitamente.

https://aws.amazon.com/rds/postgresql/features/?nc=sn&loc=2&dn=1

12.1.8. Red SAN

No se utiliza el enfoque de SAN, más bien se hace uso del servicio Amazon EBS para proveer las capacidades de almacenamiento por bloque.

https://aws.amazon.com/blogs/storage/comparing-your-on-premises-storage-patterns-with-aws-storage-services/

12.1.9. Data Center

Los centros de datos de AWS siguen procedimientos rigurosos de control de acceso en diferentes niveles que se describen en la siguiente sección.

Amazon cuenta con Centros de Operaciones de Seguridad que están distribuidos alrededor del mundo y tienen la responsabilidad de monitorear, realizar triaje y ejecutar programas de seguridad.

12.1.10. Seguridad

Nivel de Periferia

- Visitantes mediante acceso mediante autorización
- Trabajadores mediante acceso autorizado y escrudiñado 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.

12.1.11. Detalle de hardware y software

El hardware utilizado por la plataforma de PKI está detallado en las secciones 6.1.5 Servidores y 6.1.6 Almacenamiento.

El software utilizado consiste de los siguientes servicios y aplicaciones:

Amazon Virtual Private Cloud

Servicio de Amazon que permite contar con una red privada aislada dentro de la nube de AWS.

Amazon Elastic Load Balancing

Servicio de Amazon que distribuye el tráfico entrante de la plataforma PKI entre las instancias disponibles.

Amazon API Gateway

Servicio de Amazon que permite la publicación, mantenimiento, monitoreo y protección de APIs.

Amazon Cloud Watch

Servicio de Amazon que monitorea, provee datos y avisos relacionados con cambios de rendimiento, optimización de recursos, salud de la plataforma.

Amazon RDS for PostgreSQL

Servicio que prove acceso directo al software de base de datos PostgreSQL, además ofrece monitoreo, métricas, notificaciones y software patching automático.

Amazon Route 53

Servicio de DNS (Sistema de Nombres de Dominio) para registro de los dominios utilizados en los portales que expone la plataforma PKI.

Amazon Certificate Manager Private Certificate Authority

Servicio que provee una Autoridad Certificada Privada de alta disponibilidad. La AC Privada está asegurada mediante módulos de seguridad de hardware (HSM) gestionados por AWS.

Nginx

Servidor Web básico que constituye el software base de los microservicios que son parte de la plataforma PKI.

12.1.12. Ubicación y distribución de equipos en racks

Los equipos son instalados en racks administrados por Amazon.

12.1.13. Esquema de conectividad

Existen 2 formas de conectividad hacia la plataforma:

1. Acceso de usuarios

Son las personas que solicitan certificados, las cuales solamente pueden acceder al portal web público mediante un navegador. También se consideran usuarios a las Autoridades Registradoras y

Administradores de Negocio que utilizan el portal web de administración para ejecutar el proceso de validación de identidad de los solicitantes, así como gestionar parámetros.

El acceso de este grupo de usuarios es a través de internet, por lo que el tráfico de red pasa por un DNS para resolver nombres de dominio, posteriormente pasa por un balanceador de carga para direccionar el tráfico hacia la aplicación que aloja las páginas web.

2. Acceso de administradores de infraestructura

Los administradores de infraestructura están en capacidad de hacer ajustes en los servicios de AWS, instancias de servidores y aplicación a través de las consolas web que AWS pone a disposición de los usuarios. Los administradores de la infraestructura son especialistas de Montran Corporation.

El control de los servicios de AWS a través de las consolas administrativas de cada servicio es el método más seguro para acceder a los recursos de la infraestructura y facilitar la gestión. Por tal motivo, no se ha establecido ningún tipo de conectividad directa con la infraestructura.

Cabe mencionar que, para seguridad de la plataforma, se establecen reglas de acceso en un Grupo de Seguridad configurado en la VPC.

12.1.14. Topología de conectividad

La conectividad para la gestión solamente se establece a través de las consolas web de administración de cada servicio de AWS.

12.1.15. Esquema de cómputo

Los servicios que la plataforma ofrece están diseñados sobre una arquitectura de microservicios, la cual facilita el procesamiento de las peticiones de usuarios a través de diferentes aplicaciones que se ejecutan independientemente.

Los componentes que componen esta arquitectura son:

API Gateway: Es el punto de entrada a la plataforma ya que se encarga de exponer los API REST y por tanto controla que las peticiones sean dirigidas al servicio correspondiente.

Administración de Certificados: Servicio que se encarga de procesar las operaciones de certificados, tales como emitir, renovar y revocar un certificado.

Autenticación y Autorización: Servicio que realiza los procesos de autenticación (validación de credenciales de usuario) y autorización (asignación de roles de acceso).

Administración de Usuarios: Servicio cuyo objetivo es gestionar los usuarios de la plataforma y sus roles.

Notificaciones: Servicio que genera notificaciones por correo electrónico. Este servicio es extensible a otros canales de notificación como SMS.

Configuración: Servicio que mantiene la parametrización del resto de servicios de la plataforma.

Documentos: Servicio que gestiona los documentos relacionados a la plataforma, tales como documentos de certificación, acuerdos de términos y condiciones, entre otros.

Reconocimiento Facial: Servicio que lleva a cabo un proceso que busca automatizar la verificación de identidad de una persona mediante el uso de servicios de AWS basados en Machine Learning.

Sitio Web Público: Aplicación que publica el sitio web destinado para las personas que realizan las operaciones de certificados a través de Internet.

Sitio Web de Administración: Aplicación que publica el sitio web destinado para las Autoridades de Registro y Administradores de Negocio, quienes realizan tareas de verificación, control y monitoreo.

A continuación, se muestra el esquema que representa la plataforma y sus servicios.

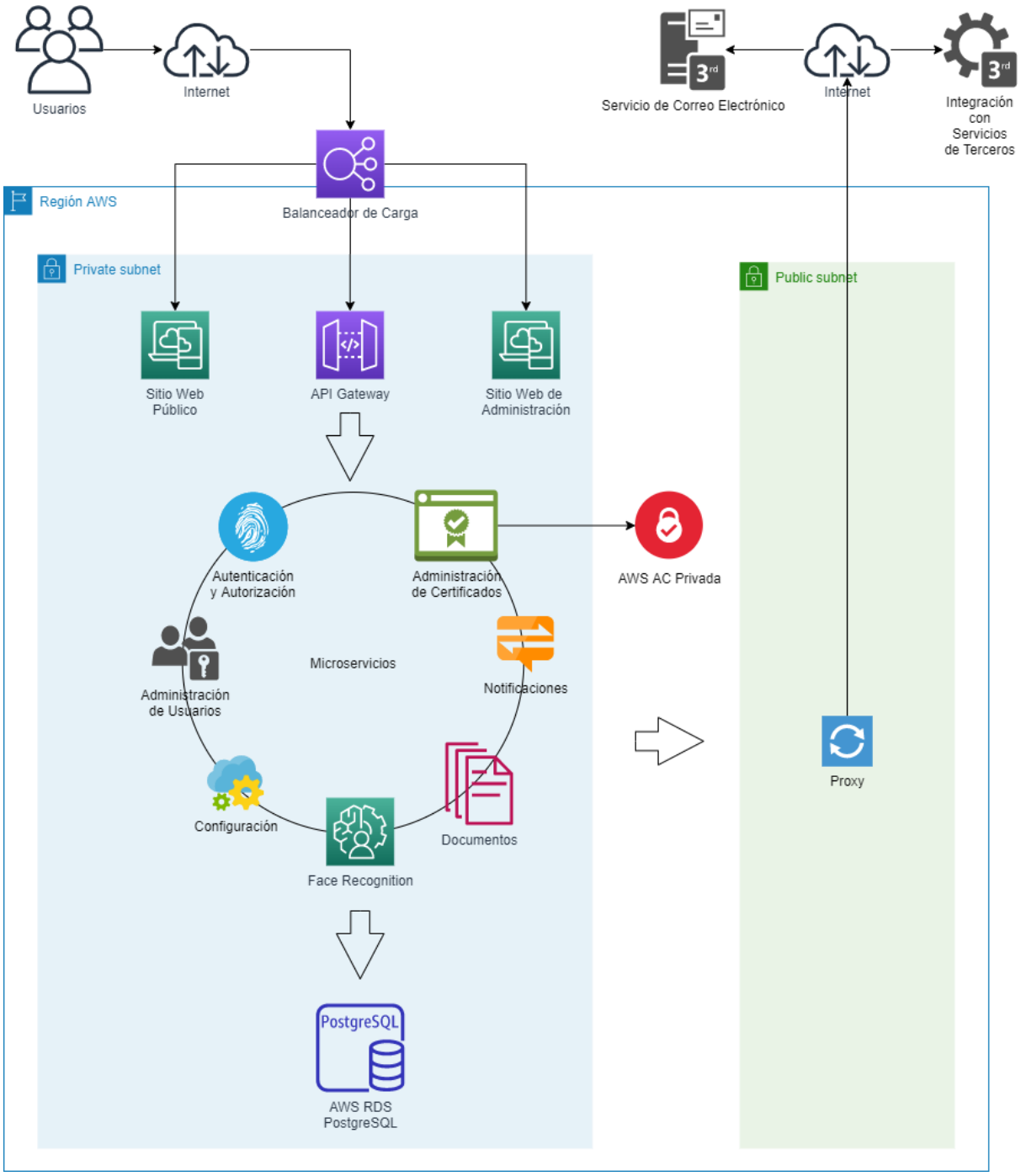


Gráfico 3. Esquema de Servicios

12.1.16. Hardware criptográfico HSM

La AC Privada de AWS está asegurada con módulos de seguridad de hardware (HSM) gestionados por AWS. Los HSMs se adhieren a los estándares de seguridad FIPS 140-2 Level 3, con el fin de almacenar de forma segura las llaves de la AC Privada.

12.1.17. Esquema de respaldos

Se utilizan respaldos automáticos programados en Amazon EBS. Adicionalmente se cuenta con espacio para snapshots que se establece en la sección 6.1.6 Almacenamiento.

Los sistemas de respaldos se establecen en la sección 6.1.7 Sistemas de Respaldo.

12.2. Sitio seguro

12.2.1. Descripción del esquema de red

Ver la sección 12.1.1 Descripción del esquema de red del Sitio Principal.

6.2.1.1 Dispositivos de seguridad de borde

Ver la sección 6.1.2 Dispositivos de seguridad de borde.

12.2.2. Almacenamiento

Ver la sección 12.1.6 Almacenamiento.

12.2.3. Red de comunicaciones

Ver la sección 12.1.4 Conectividad LAN.

13. Ubicación geográfica de cada nodo o sitio seguro

13.1. Sitio principal

El centro de datos está ubicado en la región US East (Ohio), el cual cuenta con 3 Zonas de Disponibilidad.

El sitio principal está ubicado en la primera Zona de Disponibilidad.

13.2. Sitio alterno

El centro de datos está ubicado en la región US East (Ohio), el cual cuenta con 3 Zonas de Disponibilidad.

El sitio alterno está ubicado en la segunda Zona de Disponibilidad.

14. Documentos de soporte que confirmen que se dispone de mecanismos de seguridad

14.1. Mecanismos de seguridad

14.1.1. 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.

14.1.2. 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.

14.1.3. 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.

14.1.4. 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

14.1.5. 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

14.2. 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.

14.3. Estándares y normas internacionales

14.3.1. 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.

Es importante mencionar que la versión de los certificados es X.509 versión 3.

14.3.2. 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 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 proveed 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

14.4. Componentes de seguridad perimetral

14.4.1. 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.

14.4.2. Firewall

Como parte de la arquitectura de red (ver sección 6.1.1 Descripción del esquema de red) 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.

14.4.3. Balanceadores

Se utiliza un Balanceador de Carga de Red que se lo 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 direccionarlo 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.

14.5. Esquema de seguridad perimetral

Ver sección 6.1.10. Seguridad.

14.6. 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.

Ver el siguiente link para 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 siguientes medidas:

14.7. Plan de contingencia

ArgosData opera sobre una plataforma en la nube que brinda respuesta ante desastres permitiendo centrarse en las funciones relevantes de recuperación. En la actualidad, los servicios en la nube ofrecen altos niveles disponibilidad y asegura 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 la conectividad por medio de la ayuda de técnicos que son parte del plan ofrecido por el proveedor de la nube.
- Mapeo de desastres de una forma ágil para que los servicios de emergencia puedan completar sus tareas de forma local y dirigir recursos.
- 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).
- A nivel de software, se cuenta con funciones de contingencia que permiten llevar a cabos 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 que incluyen simulaciones de diferentes situaciones. Adicionalmente, incluye detalles operativos acerca de los pasos que se deben realizar antes, durante y después de un incidente.

14.8. Sistema de control de acceso al centro de cómputo

El proveedor de la nube provee el 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 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.

14.9. Registro ingreso 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 traten de visitantes, es necesario que presenten su identificación al llegar al sitio, firmar el registro de entrada e ir acompañados del personal autorizado.

14.10. 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.

14.11. Respaldo de información de la AC

14.11.1. Esquema del sistema de respaldos

ArgosData 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.

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.

14.11.2. 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.

14.11.3. Rotación de respaldos

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

14.11.4. 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.

14.11.5. Respaldos de información

Se precisa almacenar ciertos datos personales de los solicitantes que son exclusivamente necesarios para la emisión de un certificado. Por lo que es importante el desarrollo de 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.

14.11.6. 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.