DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

VERSIÓN 2.0

DPC FIRMASEGURA S.A.S.

DECLARACIÓN DE PRÁCTICAS
DE CERTIFICACIÓN

CONTROL DE VERSIONES:

FECHA	AUTOR	VERSIÓN	DESCRIPCIÓN
20/10/2023	PAÚL ILLINGWORTH	1.0	VERSIÓN APROBADA
27/05/2024	MAURICIO PÉREZ	2.0	VERSIÓN APROBADA INICIO DE OPERACIONES

Contenido

1 Objetivo

El objetivo es describir en detalle las prácticas de certificación que la entidad sigue para garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los certificados que emite. Además, describir a detalle los lineamientos que FIRMASEGURA S.A.S. mantiene para cumplir con la normativa ecuatoriana y la norma internacional RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”.

2 Introducción

FIRMASEGURA S.A.S es una Entidad Certificadora autorizada por el ARCOTEL mediante resolución ARCOTEL-CTHB-CTDS-2023-0311 del 29 de Noviembre del 2023. Ofrece servicios de certificación de firmas electrónicas para personas naturales y representantes legales de empresas en Ecuador. La infraestructura de clave pública (PKI) utilizada por FIRMASEGURA S.A.S está basada en estándares internacionales y aplicando las mejores prácticas.

2.1 Alcance de la DPC

Esta Declaración de Prácticas de Certificación describe las prácticas de certificación que sigue FIRMASEGURA S.A.S para garantizar la seguridad y fiabilidad de los certificados emitidos a sus clientes. Incluye la descripción detallada de las prácticas y procedimientos técnicos que FIRMASEGURA S.A.S. ha implementado para asegurar la integridad, confidencialidad, autenticidad y disponibilidad de la PKI. La DPC también describe las medidas de seguridad físicas, lógicas y administrativas que FIRMASEGURA S.A.S. ha establecido para asegurar la protección de la información contenida en la PKI.

2.2 Terminología

La sección de terminología de la DPC define los términos técnicos utilizados en la declaración.

Algunos de las definiciones comunes en la terminología son:

Autoridad certificadora (CA): Una entidad confiable que emite certificados electrónicos después de verificar la identidad del titular del certificado.

Infraestructura de clave pública (PKI): Un sistema de hardware, software, personas y procedimientos que se utilizan para crear, gestionar, almacenar, distribuir y revocar certificados electrónicos.

Certificado de Firma Electrónica: Un archivo electrónico que contiene información sobre la identidad de una persona o entidad y la clave pública que se usa para encriptar y desencriptar los datos.

Certificado de clave pública (PKC): Un certificado electrónico que contiene la clave pública del titular del certificado de firma electrónica.

Certificado de revocación (CRL): Un certificado electrónico que contiene información sobre los certificados de firma electrónica revocados.

Política de Certificación (PC): Un documento que describe las prácticas y procedimientos técnicos que la CA implementa para asegurar la integridad, confidencialidad, autenticidad y

disponibilidad de la PKI.

ARCOTEL: La Agencia de Regulación y Control de las Telecomunicaciones es una entidad gubernamental en Ecuador encargada de regular y controlar los servicios de telecomunicaciones.

CA RAÍZ: Una Autoridad Certificadora Raíz es una entidad que emite certificados electrónicos a otras Autoridades Certificadoras (CA) y que es confiada por la mayoría de los dispositivos y aplicaciones para validar la autenticidad de los certificados emitidos por otras CAs.

CA Subordinada: Una Autoridad Certificadora Subordinada es una entidad que emite certificados electrónicos a usuarios finales o a otras CAs, y que confía en una CA Raíz o en otra CA Subordinada para validar la autenticidad de los certificados emitidos.

Firewall: Un firewall es un dispositivo o programa informático que se utiliza para controlar el tráfico de red y proteger los sistemas de posibles amenazas externas.

Y los acrónimos más comunes son:

PKI: Public Key Infrastructure

CA: Certificate Authority

RA: Registration Authority

CRL: Certificate Revocation List

OCSP: Online Certificate Status Protocol

SCEP: Simple Certificate Enrollment Protocol

CMS: Cryptographic Message Syntax

X.509: ITU-T standard for public key infrastructure certificates

SSL: Secure Sockets Layer

TLS: Transport Layer Security

S/MIME: Secure/Multipurpose Internet Mail Extensions

PGP: Pretty Good Privacy

GPG: GNU Privacy Guard

PKCS: Public Key Cryptography Standards

EKU: Extended Key Usage

GCP: Google Cloud Platform

OID: Object Identifier

DSA: Digital Signature Algorithm

RSA: Rivest–Shamir–Adleman encryption algorithm

ECC: Elliptic Curve Cryptography

AWS: Amazon Web Services

PEM: Privacy-Enhanced Mail

DER: Distinguished Encoding Rules

CAs: Certificate Authorities

OCSP responders: Online Certificate Status Protocol responders

HSM: Hardware Security Module

CDP: Certificate Distribution Point

AIA: Authority Information Access

CP: Certificate Policy

CPS: Certificate Practice Statement

TSA: Time-Stamp Authority

OCSP stapling: Online Certificate Status Protocol stapling

VPC: Red de nube privada virtual (VPC) es una versión virtual de una red física.

CSR: Certificate Signing Request

API: Application Programming Interface

SMS: Short Message Service

3 Descripción técnica detallada de la infraestructura y Diagrama esquemático

3.1 Detalle técnico de la infraestructura de clave pública

FIRMASEGURA S.A.S. para su infraestructura de llave pública establece la siguiente infraestructura:

3.1.1 Autoridades de Certificación (CA)

La CA raíz es la encargada de emitir certificados para las CA subordinadas y es firmada por sí misma.

3.1.2 Autoridad de Registro (AR o RA)

La AR o RA es la encargada de realizar la validación de la identidad de los solicitantes de certificados electrónicos antes de emitirlos.

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

3.1.3 Autoridad de Validación (AV o VA)

La Autoridad de Validación (AV o VA) ofrece 2 servicios para validación de un certificado:

- Validación en tiempo real mediante el protocolo OCSP.
- Validación mediante CRLs.

3.1.4 Solicitante

El solicitante puede ser cualquier usuario, sea persona natural o representante legal de una persona jurídica que necesite un certificado de firma electrónica**.**

3.1.5 Suscriptor

Los suscriptores pueden ser cualquier usuario que haya obtenido un certificado electrónico a través del servicio de certificación.

3.1.6 Custodio de claves

El Custodio de claves es la entidad encargada de la seguridad y gestión de las claves privadas de los certificados electrónicos emitidos por la CA.

3.1.7 Tercero que confía en los certificados

El Tercero que confía en los certificados es cualquier entidad que utiliza los certificados electrónicos emitidos por FIRMASEGURA S.A.S. para validar la identidad de los suscriptores o para cifrar y firmar documentos electrónicos. Esto puede incluir a proveedores, clientes o cualquier otra entidad que necesite utilizar los certificados electrónicos emitidos por FIRMASEGURA S.A.S. para sus propios fines.

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

3.2.1 FIRMASEGURA CA-1 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.

3.2.2 FIRMASEGURA SUBCA-1 Subordinada f

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 FIRMASEGURA CA-1 Raíz.

3.3 Administración de la autoridad de certificación

Procedimientos de Emisión de Certificados: La CA implementa procedimientos para la emisión de certificados de firma electrónica en formato .p12, que incluyen verificación de identidad, validación de solicitudes y generación segura de claves los cuales se detallan en el acápite 4.5.2 de este documento respectivamente.

Procedimientos de Revocación y Renovación: Se establecen procedimientos claros para la revocación y renovación de certificados en caso de pérdida o vencimiento los cuales se detallan en los acápites 4.7., 4.5.5 y 4.5.6 de este documento respectivamente.

Procedimientos de Auditoría de Seguridad: Se realizan auditorías de seguridad regulares para evaluar el cumplimiento normativo y la integridad de la infraestructura los cuales se detallan en el acápite 3.5 de este documento.

3.3.1 Roles Responsables del Control y Gestión de la Infraestructura de Clave Pública

Administrador de la CA: Este rol es responsable de la gestión general de la CA, incluyendo la administración de AWS Private CA y la infraestructura.

Operadores de la CA: Los operadores de la CA llevan a cabo las operaciones diarias, como la emisión de certificados, la renovación, la revocación y la gestión de solicitudes.

Personal de Seguridad: El personal de seguridad se encarga de garantizar la seguridad física y lógica de la infraestructura, incluyendo controles de acceso.

3.3.2 Identificación y Autenticación para cada Usuario Autorizado

Autoridades de Registro (AR): Las AR son responsables de la identificación y autenticación de los solicitantes de certificados. Se requiere que sigan procedimientos de verificación de identidad específicos.

Operadores de la CA: El personal que opera la CA debe autenticarse mediante credenciales seguras y se implementan medidas de autenticación de dos factores.

3.3.3 Roles que requieren Segregación de Funciones

Generación de Claves Privadas: La generación de claves privadas y la emisión de certificados son tareas separadas para garantizar la segregación de funciones. El personal que genera claves no emite certificados y viceversa.

Autoridades de Registro (AR): Las AR que verifican la identidad de los solicitantes no tienen permisos para emitir certificados. La emisión de certificados es realizada por operadores de la CA.

3.3.4 Controles de Personal

Verificación de Antecedentes: Todos los miembros del personal que manejan claves privadas o tienen acceso a la infraestructura se someten a una verificación de antecedentes.

Política de Confidencialidad: El personal está sujeto a políticas de confidencialidad que prohíben la divulgación no autorizada de información relacionada con la CA, mediante firma de contratos de confidencialidad.

Entrenamiento Continuo: El personal recibe capacitación al menos una vez cada seis meses sobre procedimientos de seguridad y buenas prácticas.

Control de Acceso: Se implementan controles de acceso físico y lógico para limitar el acceso solo a personal autorizado.

3.4 Roles y responsabilidades para generación y migración de llaves privadas

Se describen a continuación los roles y responsabilidades en el proceso de generación y migración de llaves privadas, garantizando la seguridad y confidencialidad de las mismas.

3.4.1 Rol Responsable de Generación de Claves Privadas:

Este rol es responsable de la generación segura de las llaves privadas utilizadas en los certificados de firma electrónica.

Responsabilidades:

Generar claves privadas utilizando métodos criptográficos seguros y aleatorios.

Almacenar y proteger las claves generadas de acuerdo con políticas de seguridad.

Requisitos de Autenticación:

Debe autenticarse mediante credenciales seguras antes de generar claves privadas.

Se requiere autenticación de dos factores para tareas críticas.

3.4.2 Rol Responsable de Migración de Llaves Privadas:

Este rol es responsable de migrar llaves privadas, por ejemplo, a un nuevo Hardware Security Module (HSM) o para la rotación de claves.

Responsabilidades:

Realizar la migración de llaves privadas siguiendo procedimientos seguros.

Garantizar que las llaves migradas se almacenan de manera segura y que las antiguas son revocadas adecuadamente.

Requisitos de Autenticación:

Debe autenticarse mediante credenciales seguras y procedimientos de autenticación adicionales al realizar migraciones.

3.5 Procesos de auditoría de seguridad

3.5.1 Definición del Plan de Auditoría:

Alcance de la Auditoría: El plan define claramente el alcance de la auditoría, que incluye la infraestructura de clave pública, políticas y procedimientos, así como cualquier otro aspecto relevante de seguridad.

Objetivos de la Auditoría: Se establecen los objetivos específicos de auditoría que son evaluar el cumplimiento de políticas, identificar vulnerabilidades y garantizar la integridad de la infraestructura.

Frecuencia de Auditoría: Se determina la frecuencia de las auditorías que serán de periodicidad anual.

Recursos Necesarios:

Personal de Auditoría: Se designará un equipo de auditores de seguridad altamente capacitados y con experiencia.

3.5.2 Programa Definido:

Plan de Auditoría Detallado: Se desarrolla un plan de auditoría detallado que incluye fechas, procedimientos, áreas específicas de evaluación y responsables de la auditoría.

Tipos de Eventos Generados: Se identifican y documentan los tipos de eventos generados que serán analizados, como registros de acceso, registros de autenticación y registros de emisión de certificados.

Análisis de Vulnerabilidades: Se lleva a cabo un análisis de vulnerabilidades para evaluar la seguridad de la infraestructura y determinar si existen vulnerabilidades que requieran medidas correctivas.

Cronograma de Auditoría: Se define un cronograma que indica cuándo se llevarán a cabo las auditorías, incluyendo fechas y duración estimada.

Recopilación de Evidencia: Se describe en detalle la recopilación de evidencia durante las auditorías, su revisión y documentación.

Informe de Auditoría: Se especifican los requisitos para la elaboración de informes de auditoría que incluyen la estructura y el contenido del informe.

Seguimiento y Medidas Correctivas: Se establece el seguimiento de hallazgos y la implementación de medidas correctivas recomendadas, con plazos definidos.

4 Descripción detallada de cada servicio propuesto y de recursos e infraestructura disponibles

4.1 Descripción y alcance detallado del portafolio de servicios propuesto y de los recursos e infraestructura disponibles para su prestación

4.1.1 Firma electrónica para personas naturales en archivo .p12:

Este servicio permite a los individuos firmar electrónicamente documentos de forma segura y confiable utilizando su propio certificado electrónico.

4.1.2 Firma electrónica para representantes legales de personas jurídicas en archivo .p12:

Este servicio permite a los representantes legales de las sociedades firmar electrónicamente documentos en nombre de la empresa utilizando su propio certificado de firma electrónica.

4.1.3 Otros servicios relacionados

Además, se ofrecerán los siguientes servicios:

- Revocación de certificados electrónicos.
- Publicación de CRL.
- Publicación de Servicios OCSP para consulta de estado de certificados.

En un futuro se brindará el siguiente servicio:

- Plataforma para firmar electrónicamente documentos.

4.1.4 Periodos de validez de los certificados

Específicamente, y en cualquier caso, se brindará el servicio de emisión de certificados de firma electrónica en formato archivo .p12 con los siguientes períodos de validez:

- Una semana
- Un mes
- Un año
- Dos años
- Tres años
- Cuatro años
- Cinco años

4.1.5 Tarifas

Las Tarifas de los servicios se publican en el sitio web www.firmaseguraec.com

4.2 Recursos e infraestructura disponibles para la prestación de cada servicio

Servidores alojados en Google Cloud Platform (GCP) con capacidad de procesamiento y almacenamiento suficientes para garantizar la disponibilidad y confidencialidad de la información de los certificados.

Sistema de gestión de certificados AWS Private CA para la emisión, renovación y revocación de certificados.

Módulo de autenticación de usuarios para validar la identidad del solicitante y garantizar la seguridad de los procesos de emisión y gestión de certificados, el cual incluye integración con el API del Registro Civil y tecnología de Inteligencia Artificial para reconocimiento de imágenes, fotografías y prueba de vida.

4.3 Mecanismos de validación: CRL, OCSP, LDAP

4.3.1 Servicio de listas de certificados revocados (CRL)

FIRMASEGURA S.A.S. publica los CRLs para permitir que las entidades de confianza verifiquen una firma electrónica que ha sido generada usando un certificado de firma electrónica emitido por FIRMASEGURA. Cada CRL contiene registros de todos los certificados revocados y es válido por 24 horas.

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

4.3.2 Servicio consulta en línea de certificados electrónicos (OCSP)

FIRMASEGURA dispone del servicio para responder a solicitudes mediante el protocolo OCSP definido en RFC 6960, este provee información en tiempo real acerca de la validez de un certificado.

La respuesta a una petición OCSP bajo el RFC mencionado 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 CA de FIRMASEGURA.

4.3.3 Servicio repositorio de certificados electrónicos (LDAP)

FIRMASEGURA no brinda el mecanismo de validación por LDAP. Como mecanismos alternos de validación seguros se utiliza CRL y OSCP descritos anteriormente.

4.4 Certificados de servidor seguro (SSL)

Nuestra plataforma web cuenta con un certificado válido de servidor seguro SSL.

4.5 Servicios de solicitud emisión, renovación, revocación y suspensión de certificados de firma electrónica

Solicitud: El solicitante debe ingresar a nuestro sitio web y completar el formulario de solicitud de certificado, proporcionando la información requerida para la validación de su identidad. Toda solicitud será a través del ingreso de información al sitio web.

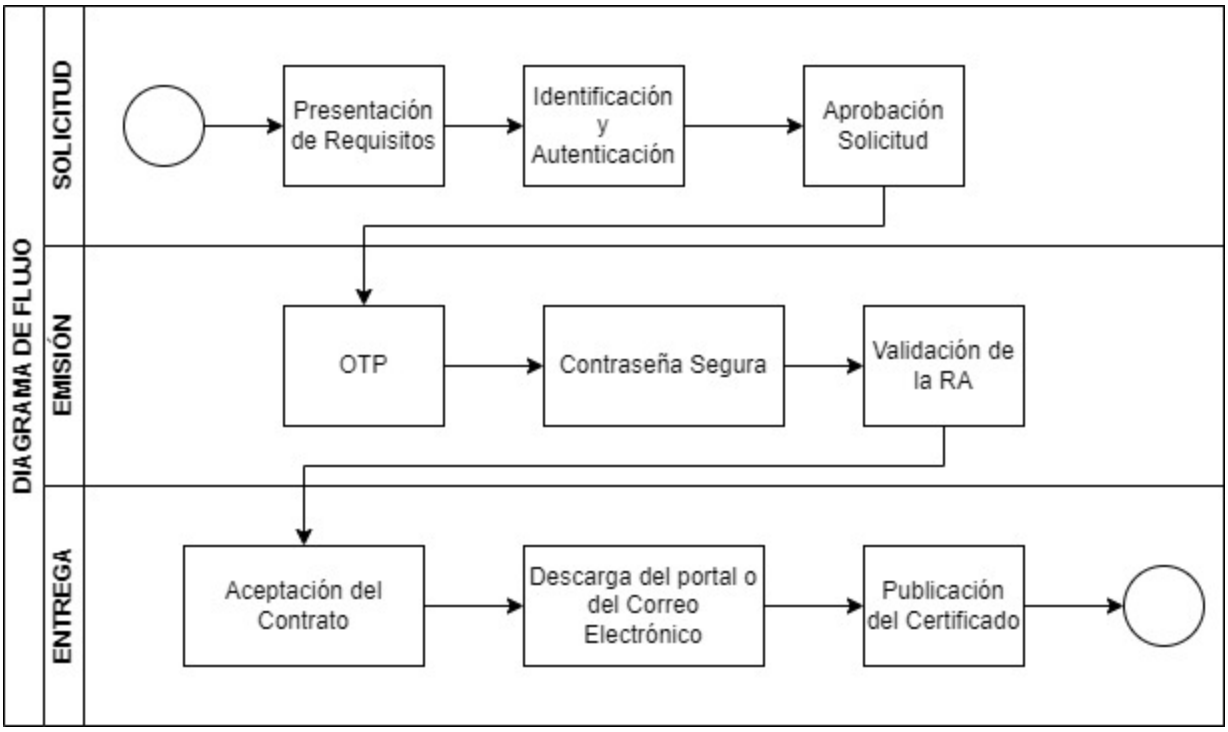
Emisión: Una vez validada la identidad del solicitante, se genera un link de descarga para el certificado de firma electrónica en formato .p12 el cual podrá descargarlo desde la plataforma, previa validación por OTP y una vez que asigne una contraseña segura, además es enviado al correo electrónico proporcionado por el solicitante. Este proceso se detalla en el acápite 4.5.2.

Renovación: El certificado se puede renovar en línea antes de su fecha de expiración siguiendo el mismo proceso de la emisión inicial.

Revocación: En caso de pérdida o compromiso del certificado, el titular debe notificar a nuestro equipo de soporte técnico para proceder con la revocación del mismo.

Suspensión: En caso de sospecha de fraude o uso indebido del certificado, se procederá con la suspensión definitiva del mismo.

A continuación se muestra el diagrama de flujo del proceso general:



En los siguientes numerales se detalla cada uno de los procesos:

4.5.1 Solicitud de certificados

4.5.1.1 Quién puede solicitar un certificado

Los requisitos que debe reunir un Solicitante dependerá del tipo de certificado solicitado y estarán recogidos en la Política de Certificación de cada tipo de certificado concreto.

4.5.1.2 Proceso de solicitud de certificados

El Solicitante deberá ponerse en contacto con FIRMASEGURA S.A.S. por cualquiera de los canales habilitados para este proceso, ya sea por su sitio web, de manera presencial en sus locales u oficinas, o por medio de unos de sus Terceros Vinculados, para gestionar la solicitud del certificado, en todos los casos la solicitud finalmente se registrará en la plataforma web.

La CA proporcionará al Solicitante la siguiente información:

- Documentación necesaria para presentar para la tramitación de su solicitud y para verificar la identidad del Suscriptor y del Solicitante.

- Disponibilidad para realizar el proceso de registro.

- Información sobre el proceso de emisión y revocación, de la custodia de la clave privada, así como de las responsabilidades y las condiciones de uso del certificado y del dispositivo.

- Acceder y aceptar las condiciones de contratación.

4.5.1.3 Rango de validez del certificado de firma electrónica

En concordancia con lo expuesto en el Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, la duración de los certificados de firmas electrónicas es:

"La duración del certificado de firma electrónica se establecerá contractualmente entre el titular de la firma electrónica y la entidad certificadora de información o quien haga sus veces. En caso de que las partes no acuerden nada al respecto, el certificado de firma electrónica se emitirá con una validez de dos años a partir de su expedición. Al tratarse de certificados de firma electrónica emitidos con relación al ejercicio de cargos públicos o privados, la duración del certificado de firma electrónica podrá ser superior a los dos años, pero no podrá exceder el tiempo de duración de dicho cargo público o privado a menos que exista una de las prórrogas de funciones establecidas en las leyes."

En todo caso, nuestros contratos tendrán el periodo de validez a disposición del cliente, siendo estos desde una semana hasta 5 años conforme se detalla en el acápite 4.1.4 del presente documento.

4.5.1.4 Identificación y Autenticación

Es responsabilidad de la CA realizar de forma fehaciente la identificación y autenticación del Suscriptor. Este proceso deberá ser realizado previamente a la emisión del certificado, conforme se detalla en el numeral 4.5.1.4 del presente documento.

4.5.1.5 Aprobación o denegación de las solicitudes de certificados

Una vez realizada la solicitud de certificado, la CA deberá verificar la información proporcionada por el Solicitante incluyendo la validación de la identidad del Solicitante.

Esta validación se realizará mediante la comparación de los datos y documentos suministrados por el solicitante.

La validación de la identidad del solicitante será biométrica y documental, mediante el registro y procesamiento en la plataforma web de la CA conforme se detalla en el acápite 4.5.1.4 del presente documento.

Si la información no fuese correcta, la CA deberá denegar la petición, contactando con el Solicitante, y el Firmante o el Custodio de claves para comunicarles el motivo.

Si la información es correcta, y en el caso de la emisión de un Certificado de persona natural, se procederá a la firma del instrumento jurídico vinculante entre el Suscriptor y FIRMASEGURA S.A.S. En el caso de la emisión de Certificados para Representante Legal de una persona jurídica y para la Función Pública, FIRMASEGURA S.A.S. verificará que el instrumento jurídico existe y que ha sido firmado, siendo responsabilidad del Solicitante verificar el cargo, título o rol declarado, así como, en su caso, su vinculación con la misma.

Se procederá entonces a la emisión del certificado.

4.5.2 Emisión de certificados

4.5.2.1 Acciones de la CA durante la emisión de los certificados

Una vez aprobada la solicitud se procederá a la emisión del certificado, que deberá ser entregado de forma segura al suscriptor.

Se proporcionará un código de autenticación (OTP) al Suscriptor que deberá presentar para proceder con la generación del certificado, en la que se incluye la generación de las claves, la emisión del certificado y la descarga de ambos en formato PKCS #12 protegidos con una contraseña segura que él suscriptor debe

establecer.

La RA verificará el contenido de la petición de certificado, y si la verificación es correcta validará la petición.

La RA enviará a la CA por un canal seguro el CSR en junto con el resto de los datos verificados que están contenidos en el certificado. Se procederá entonces a la generación del certificado en un procedimiento que utilizará protección contra falsificación y mantendrá la confidencialidad de los datos intercambiados.

Entrega del certificado: El certificado emitido será enviado a la RA, que lo pondrá a disposición del Suscriptor y podrá ser descargado desde su correo electrónico o desde el portal web para lo cual se le entregará el link de descarga del certificado.

4.5.2.2 Notificación al Suscriptor de la emisión del certificado

La RA notificará al Suscriptor la emisión del certificado y el método de descarga si es necesario.

4.5.3 Aceptación del certificado

4.5.3.1 Forma en la que se acepta el certificado

El certificado se aceptará en el momento que el instrumento jurídico vinculante entre el Suscriptor y FIRMASEGURA S.A.S. haya sido suscrito y el certificado haya sido entregado al Suscriptor, ya sea personal o telemáticamente.

Como evidencia de la aceptación, quedará constancia electrónica de la aceptación del Suscriptor. El certificado se considerará válido a partir de la fecha en que se dio la aceptación.

4.5.3.2 Publicación del certificado

Una vez que el certificado haya sido emitido y haya sido aceptado por el Suscriptor, el certificado podría ser publicado en los repositorios de certificados que se consideren necesarios.

4.5.4 Uso de las claves y el certificado

4.5.4.1 Uso de la clave privada y del certificado por el Suscriptor

Los certificados podrán ser utilizados según lo estipulado en esta DPC, en la Política de Certificación correspondiente. El par de claves emitido por la CA no están restringidas para su uso, de acuerdo con el estándar X509 V3 que por sus características son multi propósito: Firma electrónica, Sin Repudio, Cifrado de Clave.

Las extensiones Key Usage y Extended Key Usage podrán ser utilizadas para establecer límites técnicos a los usos de la clave privada del certificado correspondiente. La aplicación de estos límites dependerá en gran parte de su correcta implementación por aplicaciones informáticas, quedando su regulación fuera del alcance de este documento.

4.5.4.2 Uso de la clave pública y del certificado por los terceros que confían en los certificados

Los terceros que confían en los certificados podrán utilizar los certificados para aquello que establece la presente DPC y la Política de Certificación correspondiente.

Es responsabilidad de los terceros verificar el estado del certificado mediante los servicios ofrecidos por FIRMASEGURA S.A.S. concretamente para ello y especificados en el presente documento.

4.5.5 Renovación de certificados sin cambio de claves

Dentro de nuestros servicios por motivos de garantizar la seguridad e integridad del proceso no se contempla esta opción de renovar certificados sin cambios de claves.

4.5.6 Renovación con cambio de claves

FIRMASEGURA S.A.S. Autoridad de Certificación enviará una notificación de recordatorio de caducidad del certificado por correo electrónico al Suscriptor 30, 15 y 5 días antes de la fecha de caducidad del certificado.

El Proceso de renovación será en línea, siguiendo el mismo procedimiento que para la emisión del certificado.

4.5.7 Tramitación de las peticiones de renovación en línea

Se realizarán los siguientes pasos:

- Se notificará al Suscriptor por correo electrónico que esté habilitado para renovar su certificado.
- El Suscriptor deberá acceder a la página web de renovación de su certificado en www.firmaseguraec.com
- Deberá autenticar su identidad según lo descrito y especificado en esta DPC.
- Se realizarán las mismas validaciones y se solicitarán los mismos requisitos que en la solicitud inicial de emisión de certificado.
- El proceso será idéntico al de la solicitud inicial.

4.5.8 Notificación de la emisión del certificado renovado

La CA notificará al Firmante que el certificado ha sido renovado al finalizar correctamente el proceso.

4.5.9 Publicación del certificado renovado

Una vez el certificado haya sido renovado, el nuevo certificado podría ser publicado en los repositorios de certificados que se consideren necesarios reemplazando al certificado anterior, siempre que el Suscriptor o el Firmante no se hubiera opuesto.

4.6 Modificación de certificados

En caso de necesidad de modificar algún dato, la RA deberá proceder a la revocación y el suscriptor deberá seguir el proceso de solicitud de emisión de un nuevo certificado.

4.7 Revocación de certificados

La revocación de un certificado supone la pérdida de validez de este y no podrá ser reversado. Las revocaciones tienen efecto desde el momento en que aparecen publicadas en la CRL.

4.7.1 Circunstancias para la revocación

Un certificado podrá ser revocado debido a las siguientes causas:

a) Circunstancias que afectan a la información contenida en el certificado:

- Comprobación de que los datos contenidos en la solicitud del certificado son falsos o incorrectos.

• Modificación de cualquier dato contenido en el certificado.

• Extinción de la personalidad jurídica, o disolución de la entidad sin personalidad jurídica.

b) Circunstancias que afectan a la seguridad de la clave privada o del certificado:

• Compromiso o sospecha de compromiso de la clave privada o de la infraestructura o sistemas de la CA, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.

• Infracción por parte de la CA o de la RA de los requisitos previstos en los procedimientos de gestión de certificados establecidos en la DPC o en la PC correspondiente.

• Compromiso o sospecha de compromiso de la seguridad de la clave privada o del certificado.

• Acceso o utilización no autorizados por un tercero de la clave privada del certificado.

• El incumplimiento por parte del Suscriptor de las normas de uso del certificado expuestas en la presente DPC, en la PC correspondiente o en el instrumento jurídico vinculante entre la CA y el Suscriptor.

• En caso de que se advierta que los mecanismos criptográficos utilizados para la generación de la clave privada o el certificado no cumplen los estándares de seguridad mínimos necesarios para garantizar su seguridad.

c) Circunstancias que afectan a la seguridad del dispositivo criptográfico:

• Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.

• Pérdida o inutilización por daños del dispositivo criptográfico.

• Acceso no autorizado por un tercero a los datos de activación del dispositivo criptográfico.

• Incumplimiento por parte del Suscriptor de las normas de uso del dispositivo criptográfico expuestas en la presente DPC, en la PC correspondiente o en el instrumento jurídico vinculante entre la CA y el Suscriptor.

d) Circunstancias que afectan al Suscriptor:

• Finalización de la relación jurídica entre la CA y el Suscriptor.

• Modificación o extinción de la relación jurídica subyacente o causa que permitió la emisión del certificado al Firmante.

• Oposición o modificación, por parte del Suscriptor, de los datos contenidos en el fichero de datos de carácter personal de FIRMASEGURA S.A.S.

• Infracción por el Solicitante del certificado de los requisitos y obligaciones establecidos para la solicitud de este.

• Infracción por el Suscriptor, de sus obligaciones y responsabilidades establecidas en la presente DPC, en la PC correspondiente o en el instrumento jurídico correspondiente vinculante entre la CA y el Suscriptor.

• Capacidad modificada judicialmente o incapacidad sobrevenida, total o parcial,

• El fallecimiento del Firmante.

• Solicitud escrita por Suscriptor.

e) Otras circunstancias:

• Resolución judicial o administrativa que lo ordene.

• Cese de la actividad de una RA, salvo que expresamente se decida lo contrario (revocación masiva de todos de los certificados vigentes emitidos por esa RA).

• Por cualquier otra causa especificada en la presente DPC o en la PC correspondiente.

4.7.2 Quién puede solicitar la revocación

Pueden solicitar la revocación de un certificado:

1. El Suscriptor, quien deberá solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.

2. FIRMASEGURA S.A.S., que deberán solicitar la revocación de un certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.

3. Cualquier otra persona podrá solicitar la revocación de un certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.

Podrán tramitar la solicitud de revocación del certificado:

- El Suscriptor, en los casos de revocación de certificados en línea.

- Los operadores autorizados de FIRMASEGURA S.A.S. (Responsables de Revocación).

En todo caso, al tiempo de revocarse el certificado, se enviará un comunicado por correo electrónico al Suscriptor, especificando la fecha y la hora y el motivo de la revocación.

4.7.3 Procedimientos de solicitud de revocación

Existen distintas alternativas para solicitar la revocación de un certificado.

El suscriptor recibirá una comunicación del sistema informando que se ha producido la revocación del certificado, indicando la fecha, la hora y la causa de la revocación.

4.7.4 Procedimiento de revocación en línea

Para los tipos de certificados que recojan en su Política de Certificación la revocación de certificados en línea, FIRMASEGURA S.A.S. pondrá a disposición del Suscriptor el email: revocacion@firmaseguraec.com para realizar la solicitud.

Todas las revocaciones son efectivas desde el momento en que son publicadas en la CRL de la CA. Este proceso asume la aceptación explícita de la tramitación de la solicitud de revocación y las consecuencias de ésta.

Una vez aceptada la tramitación, el certificado será inmediatamente revocado.

La RA enviará una comunicación del sistema informando que se ha producido la revocación del certificado.

Requisitos para Persona natural:

1. Llenar la solicitud de revocación que se encuentra en https://firmaseguraec.com/revocatoria/. (Esta puede ser firmada de forma física o electrónica).
2. Copia digital de cédula del solicitante. “Ambos lados”
3. Opcional: Serial del certificado.
4. Enviar al mail con ASUNTO: Revocatoria PN y “Número de Cédula”. Ejemplo: “Revocatoria-PN-1001265478”.

Requisitos para Representante Legal:

1. Llenar la solicitud de revocación que se encuentra en https://firmaseguraec.com/revocatoria/. (Esta puede ser firmada de forma física o electrónica).
2. Copia digital de cédula del solicitante. “Ambos lados”
3. Serial del certificado: Opcional
4. En caso de ser por POR CAMBIO DE REPRESENTANTE LEGAL se deberá adjuntar la justificación como puede ser la carta de renuncia o nuevo nombramiento debidamente registrados y legalizados.
5. Enviar al mail con ASUNTO: Revocatoria RL y “Número de RUC de la empresa”. Ejemplo: “Revocatoria-RL-1001265478001”.

Horario para atender una solicitud de Revocación:

El firmante deberá ponerse en contacto con la Autoridad de Registro en donde tramitó el certificado (FIRMA SEGURA S.A.S) únicamente por correo electrónico, estos requerimientos serán atendidos en horarios laborables de 8:00 horas a 17:00 horas, En caso de ser fin de semana se procederá atender el requerimiento en el tiempo establecido y permitido en la normativa vigente.

4.7.5 Procedimientos internos de revocación

FIRMASEGURA S.A.S., y las Autoridades de Registro podrán solicitar la revocación de certificados mediante procedimientos internos.

Un operador autorizado de FIRMASEGURA S.A.S. (Responsable de Revocación) deberá identificar y autenticar al solicitante de la revocación mediante los procedimientos que considere oportunos, y comprobar que la causa comunicada se corresponde con alguna de las circunstancias anteriormente indicadas.

Una vez correctamente identificado el solicitante de la revocación y comprobada la causa comunicada, el operador procederá a tramitar la solicitud de revocación.

4.7.6 Plazo en el que la CA debe procesar la solicitud de revocación

El tiempo máximo desde la recepción de la solicitud de revocación hasta su confirmación y tramitación será de 24 horas. Si en ese tiempo no se puede confirmar la solicitud de revocación, ésta no será tramitada.

Una vez que la solicitud de revocación haya sido confirmada y debidamente tramitada, será procesada por la CA inmediatamente.

4.7.7 Obligación de verificación de las revocaciones por los terceros que confían en los certificados

La verificación del estado de los certificados es obligatoria para cada uso de los certificados, ya sea mediante la consulta de la CRL o del servicio OCSP.

4.7.8 Frecuencia de emisión de las CRL

La CRL de los certificados de entidad final se emite cada 24 horas.

4.7.9 Tiempo máximo entre la generación y la publicación de las CRL

Una vez emitida la CRL de los certificados de CA, ésta se publica y actualiza de forma automática.

4.7.10 Disponibilidad de sistemas en línea de verificación del estado de los certificados

FIRMASEGURA S.A.S. tiene disponible el sistema en línea de verificación del estado de los certificados, el cual está disponible las 24 horas del día, 7 días de la semana, con un porcentaje de disponibilidad de 99.97% de acuerdo a estándares internacionales del servicio.

4.7.11 Requisitos de comprobación de revocación en línea

Para el uso del sistema de comprobación de revocación en línea por CRL, de libre acceso, deberá considerarse lo siguiente:

- Se deberá comprobar el estado de revocación del certificado de entidad final en la última CRL emitida y publicada por la SUBCA-1 Subordinada de FIRMASEGURA S.A.S., que podrá descargarse en la dirección URL contenida en el propio certificado, en su extensión CRL Distribution Points.

- Se deberá comprobar que cada CRL esté vigente (con un valor del campo nextUpdate posterior a la fecha y hora actuales) y firmada por la CA que ha emitido el certificado que se quiere validar.

- Los certificados revocados que expiren son retirados de las CRL.

4.8 Servicios de información del estado de los certificados

4.8.1 Características operativas

FIRMASEGURA S.A.S. ofrece un servicio gratuito de publicación en Web de Listas de Certificados Revocados (CRL), sin restricciones de acceso, en el sitio http://crl.firmaseguraec.com/crl/, así como en los certificados, en su extensión CRL Distribution Points.

FIRMASEGURA S.A.S. ofrece un servicio gratuito de validación de certificados por medio del protocolo OCSP, sin restricciones de acceso, en el sitio http://ocsp.firmaseguraec.com, así como en los certificados, en su extensión Authority Information Access.

Adicionalmente, FIRMASEGURA S.A.S. puede ofrecer otros servicios comerciales de Validación de certificados.

4.8.2 Disponibilidad del servicio

La información relativa al estado de los certificados estará disponible en línea las 24 horas del día, los 7 días de la semana, con un porcentaje de disponibilidad de 99.97% de acuerdo a estándares internacionales del servicio.

En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de FIRMASEGURA S.A.S., éste realizará los mayores esfuerzos para asegurar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo de 24 horas para lo cual se ha establecido el proceso de contingencia de GCP conforme se lo puede revisar en el acápite 8.9.2 del presente documento.

En el caso del cese de actividad de la CA de FIRMASEGURA S.A.S. sin transferencia de la gestión de los certificados emitidos a otro Ente de Certificación, se realizará una revocación masiva de todos los certificados vigentes emitidos y se emitirá y publicará una última CRL que tendrá un valor del campo next Update igual a la fecha y hora UTC 31/12/9999 23:59:59 y contendrá todos los certificados revocados, incluyendo aquéllos que hubiesen expirado y la extensión X.509ExpiredCertsOnCRL. Esta última CRL de la CA de FIRMASEGURA S.A.S. estará disponible durante al menos 15 años desde su emisión, mientras que el servicio OCSP de la CA de FIRMASEGURA S.A.S. dejará de estar disponible.

La provisión de la información sobre el estado de los certificados queda garantizada en el caso de cese de la actividad de FIRMASEGURA S.A.S. como CA, mediante la transferencia de la gestión de los certificados emitidos a otro Ente de Certificación, quien conservará la información relativa a los servicios de certificación prestados hasta entonces por FIRMASEGURA S.A.S., o mediante la comunicación a la administración competente de la información relativa a todos los certificados cualificados expedidos cuya vigencia habrá sido extinguida, para que se haga cargo de su custodia.

4.8.3 Finalización de la suscripción

La suscripción del certificado finalizará en el momento de expiración o revocación del certificado.

4.9 Procedimientos para la validación de la identidad del solicitante y la verificación de la información proporcionada

Para la identificación de la persona natural o del Representante Legal de la Persona Jurídica se exigirá validar su identidad lo cual que se trata de comprobar ser quien dice ser y se acreditará mediante el Cédula de Identidad, el pasaporte u otros medios admitidos en derecho.

El proceso de validación se realiza mediante validación biométrica, documental y de cualquier otro medio que garantice en derecho la identidad del suscriptor.

La RA se reserva el derecho de no aprobar la solicitud del certificado si considera que la documentación aportada no es suficiente para la validación.

La persona natural deberá declarar que sus datos de identidad y otros atributos personales incluidos en la misma son correctos, mediante su aceptación por medios electrónicos.

La RA registrará los datos y documentos relativos a la identificación y autenticación del Solicitante y del Firmante del certificado de firma electrónica, o del Solicitante y del Custodio de claves del certificado.

4.9.1 Validación de la Identidad del Solicitante

Verificación de Documentos de Identidad: El solicitante debe proporcionar documentos de identidad válidos, como una cédula de identidad, pasaporte u otro documento emitido por el Registro Civil del Ecuador. La RA verifica la autenticidad de estos documentos.

Entrevista en Persona: En algunos casos, especialmente para certificados que se utilizarán en aplicaciones de alto riesgo, la RA puede requerir bajo su criterio que el solicitante se presente en persona para una entrevista de validación de identidad. Durante esta entrevista, se verifica la correspondencia de la persona con los documentos presentados y se toma una fotografía para comparación.

Verificación de Biometría Facial: La tecnología biométrica facial se utilizará para comparar la fotografía del solicitante con la fotografía de su documento de identidad. Esto ayuda a confirmar que la persona que solicita el certificado es la misma que aparece en el documento.

Además, se realizará una verificación de la información proporcionada por el solicitante con fuentes de información confiables y que garantice la autenticidad de los datos.

Para la identificación y autenticación de la persona jurídica identificada en el certificado de firma electrónica se validará conforme a los siguientes puntos:

La RA verificará los siguientes datos de la persona jurídica (Suscriptor):

- La denominación o razón social de la persona jurídica.

- Registro Único de Contribuyentes (RUC)

- Los datos relativos a la constitución y personalidad jurídica.

- Los datos relativos a la extensión y vigencia de las facultades de representación del Solicitante.

La RA podrá verificar los datos indicados según los siguientes procedimientos:

- Mediante los documentos, públicos si resultan exigibles, que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible.

- Mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

La RA se reserva el derecho de no aprobar la solicitud del certificado si considera que la documentación aportada no es suficiente o adecuada para la comprobación de los datos.

El Solicitante deberá aceptar que sus datos de identidad y los datos de la persona jurídica incluidos en la misma son correctos.

La RA registrará los datos y documentos relativos a la identificación y autenticación de la persona jurídica identificada en el certificado de firma electrónica.

Para garantizar la precisión de los datos proporcionados la CA se integrará con el Registro Civil de Ecuador para verificar la información del solicitante, como su nombre completo, fecha de nacimiento, estado civil, fotografía del documento, código dactilar, esta integración se realizará mediante la conexión con los servicios contratados con la entidad pública a través de sus API’s definidas para el efecto.

De igual manera para validar información de personas naturales con RUC o Representantes Legales de Personas jurídicas se realizará integraciones con servicios que publique el Servicio de Rentas Internas.

Para personas jurídicas bajo el control de la Superintendencia de Compañías se realizará integraciones con datos o servicios públicos de esta entidad con el fin de validar la información presentada.

4.10 Políticas de retención de registros y de privacidad de la información del solicitante

Retención de registros: Se mantendrá un registro de todas las transacciones relacionadas con los certificados electrónicos emitidos, incluyendo la información del solicitante y la fecha de emisión. Estos registros se conservarán durante el tiempo mínimo de dos años conforme lo exige la normativa aplicable y en el caso de certificados con una validez o vigencia mayor se conservarán por el tiempo de vigencia del certificado más dos meses, es decir si un certificado tiene vigencia de 1 mes se conservarán sus registros por 2 años, y si el certificado tiene vigencia de 5 años se conservarán sus registros por 5 años y 2 meses.

Privacidad de la información del solicitante: La información proporcionada por el solicitante será tratada

con estricta confidencialidad y sólo se utilizará para los fines previstos en esta DPC. No se compartirá con terceros, salvo requerimiento de autoridades competentes en cumplimiento de la normativa aplicable, cuando los datos deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la normativa vigente. Las autoridades competentes a las cuales se les podrá suministrar datos son principalmente, pero no limitadas a: Agencia de Regulación y Control de las Telecomunicaciones, Fiscalía General del Estado, Autoridad de Protección de Datos Personales, y Ministerio de Telecomunicaciones y Sociedad de la Información.

4.11 Propósitos y usos de los certificados

Los certificados emitidos por FIRMASEGURA S.A.S serán utilizados exclusivamente para la firma electrónica de documentos y archivos electrónicos. FIRMASEGURA S.A.S no garantiza ni se hace responsable de cualquier otro propósito o uso de los certificados emitidos.

4.12 Responsabilidades y obligaciones de los usuarios de certificados

Los usuarios de certificados emitidos por FIRMASEGURA S.A.S tendrán las siguientes responsabilidades y obligaciones:

• Utilizar el certificado únicamente para los fines previstos.

• Mantener la seguridad de las claves privadas asociadas al certificado.

• Notificar inmediatamente a FIRMASEGURA S.A.S en caso de sospecha de uso no autorizado o compromiso de la clave privada asociada al certificado.

5 Autoridades de registro (AR)

5.1 Autoridad de registro o Registradoras (ARs o RAs)

La Autoridad de Registro (AR) es una entidad que actúa como intermediaria entre los solicitantes de certificados digitales y la Autoridad de Certificación (AC).

Las Registradoras (RAs) son agentes autorizados por la AR para realizar tareas específicas de autenticación y verificación de identidad de los solicitantes.

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 fuentes adicionales de información.
- Validar documentos que sustentan la información
- Obtener información a partir de los servicios del Registro Civil del Ecuador o de otras Instituciones públicas.
- Aprobar o rechazar el registro de una solicitud.

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

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

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

6.1 Sitio seguro principal

6.1.1 Descripción del esquema de red

La arquitectura de red es diseñada utilizando los recursos e infraestructura de GCP (Google Cloud Platform) junto a Cloudflare y AWS. Para el correcto funcionamiento de la misma se disponen los siguientes recursos de conectividad:

Cloudflare WAF: Capa de seguridad que filtra todo el tráfico que se dirige hacia GCP. La comunicación entre ambos servicios es mediante claves públicas y privadas evitando falsos intermediarios.

Cloud External IP Addresses: Servicio para reserva de direcciones IP públicas.

Cloud Load Balancing: Controla el tráfico entrante por la IP pública y lo redirige a los servicios solicitados que se encuentren habilitados por reglas del firewall.

Cloud Firewall Rules: Conjunto de reglas de seguridad que controlan la comunicación externa e interna de los servicios

Cloud Nat: Permite que ciertos recursos en Google Cloud creen conexiones salientes a Internet o a otras redes de nube privada virtual.

Cloud Router: Intercambiador de rutas de forma dinámica entre la nube privada virtual (VPC) y la red de intercambio de tráfico mediante el Protocolo de puerta de enlace fronteriza

Region GCP: Es una ubicación geográfica específica donde se pueden alojar recursos. Cada región tiene varias zonas separadas físicamente.

Zone GCP: Es un área de implementación dentro de una región. El nombre completo de una zona está compuesto por <region>-<zone> .

VPC: Red de nube privada virtual (VPC) es una versión virtual de una red física que se implementa dentro de la red de producción de Google.

API Registro Civil: API proporcionada por el Registro Civil de Ecuador para consulta de datos y biometría.

API Email: API para envío de notificaciones por emails generados por la RA.

API SMS: API para envío de OTP por sms generados por la RA.

API AWS Private CA: API para comunicación con la CA proveída por AWS.

API Image Recognition: API para análisis de imágenes, detección de etiquetas, textos y rostros.

6.1.2 Dispositivos de seguridad de borde

GCP se encarga completamente de administrar la seguridad de borde de la infraestructura desplegada.

La seguridad física en los centros de datos de Google es un modelo de seguridad en capas. La seguridad física incluye protecciones como tarjetas de acceso electrónicas personalizadas, alarmas, barreras de acceso para vehículos, cercas perimetrales, detectores de metales y sistemas biométricos.

Acceso

Solo se puede acceder al centro de datos a través de un pasillo de seguridad en el que se implementan controles de acceso de varios factores, con credenciales de seguridad y datos biométricos. Solo los empleados autorizados con funciones específicas pueden ingresar. Menos del uno por ciento de los empleados de Google ingresarán alguna vez en centros de datos.

Energía

Para mantener el funcionamiento las 24 horas, todos los días y proporcionar servicios sin interrupciones, los centros de datos tienen sistemas de alimentación redundantes y controles de entorno. Cada componente fundamental tiene una fuente de alimentación principal y una alternativa, ambas con igual potencia. Los generadores de respaldo pueden proporcionar suficiente energía eléctrica en caso de emergencia, para que cada centro de datos funcione a máxima capacidad.

Los sistemas de enfriamiento mantienen una temperatura de funcionamiento constante en los servidores y en otros tipos de hardware, lo que reduce el riesgo de interrupciones del servicio, a la vez que minimiza el impacto ambiental.

Detección de incendios y prevención

El equipo de detección y extinción de incendios ayuda a evitar daños en el hardware. Los detectores de calor, detectores de incendios y detectores de humo activan alarmas de sonido y visuales en las consolas de operaciones de seguridad y en los puestos de supervisión remotos.

6.1.3 Acceso a servicios desde internet

Al ser una nube todo acceso es por internet. Cada usuario con acceso a GCP tiene una cuenta asociada a su correo empresarial con factor de doble autenticación.

Cada usuario tiene un rol específico asignado junto a sus permisos por medio de IAM.

En cuanto a acceso a usuarios finales únicamente tendrán acceso a servicios públicos como (OCSP, CRL, solicitud de certificados). Los servicios internamente trabajan con redes privadas sin acceso entrante desde internet.

6.1.4 Conectividad LAN

GCP trabaja con VPC la cual permite configurar interfaces de redes para comunicación de los diferentes componentes por medio de sus IPs privadas.

Las redes de VPC tienen las siguientes propiedades:

- Las redes de VPC, incluidas sus reglas de firewall y rutas asociadas, son recursos globales. No están asociadas con ninguna región o zona en particular.
- Las subredes son recursos regionales.
- Cada subred define un rango de direcciones IPv4. Las subredes en redes de VPC de modo personalizado también pueden tener un rango de direcciones IPv6.
- El tráfico desde y hacia las instancias puede controlarse mediante las reglas de firewall de la red. Las reglas se implementan en las VM. Por lo tanto, el tráfico solo se puede controlar y registrar a medida que sale o llega a una VM.
- La administración de red se puede proteger mediante roles de administración de identidades y accesos (IAM).

Rendimiento de la red

Por lo general, Google Cloud mide las latencias de ida y vuelta de menos de 55 µs en el percentil 50 y las latencias finales de menos de 80 µs en el percentil 99 entre instancias de VM c2-standard-4 en la misma zona.

Pérdida de paquetes

Google Cloud hace un seguimiento de la pérdida de paquetes entre regiones mediante la medición regular de la pérdida de ida y vuelta entre todas las regiones. El objetivo es que el promedio global de esas mediciones sea inferior al 0.01%.

Metodología: Un sistema de sondeo de VM a VM de caja negra supervisa la pérdida de paquetes para cada par de zonas mediante pings y agrega los resultados en una métrica de pérdida global. Se realiza un seguimiento de esta métrica con un período de un día.

6.1.5 Servidores

Los servicios para el funcionamiento de la CA se encuentran sobre contenedores docker que se ejecutan en máquinas virtuales de Google compute engine tipo N2 bajo la administración de Google kubernetes engine.

Nodo 1:

Hardware:

Máquina virtual (VM) en GCP

Procesador: 4 vCPUs Intel Cascade Lake Xeon Gold 6268CL 2.8 GHz

RAM: 16 GB de RAM

Almacenamiento: 100 GB disco persistente equilibrado. IOPS máximas de escritura:

80,000. Capacidad de procesamiento máxima de escritura y lectura (MiBps): 1,200

Software:

Sistema operativo Linux (Container-Optimized OS con Containerd).

Firewall configurado para permitir el tráfico de certificados y los puertos necesarios para la operación de la CA.

Nodo 2:

Hardware:

Máquina virtual (VM) en GCP

Procesador: 4 vCPUs Intel Cascade Lake Xeon Gold 6268CL 2.8 GHz

RAM: 16 GB de RAM

Almacenamiento: 100 GB disco persistente equilibrado. IOPS máximas de escritura:

80,000. Capacidad de procesamiento máxima de escritura y lectura (MiBps): 1,200

Software:

Sistema operativo Linux (Container-Optimized OS con Containerd).

Firewall configurado para permitir el tráfico de certificados y los puertos necesarios para la operación de la CA.

En cuanto a base de datos. Estas se encuentran bajo el servicio de Google Cloud SQL que se encarga de la ejecución de la misma.

Hardware:

Procesador: 2 vCPU.

Memoria RAM: 16 GB.

Capacidad de procesamiento de la red (MB/s): 500

Capacidad de procesamiento del disco (MB/s): Lectura: 9.6 de 240.0, Escritura: 9.6 de 240.0

IOPS: Lectura: 600 de 15,000, Escritura: 600 de 15,000

Almacenamiento en disco: 20 GB de almacenamiento (iniciales) en disco sólido (SSD) con auto incrementación de espacio según necesidad de almacenamiento.

Software:

Motor de base de datos: PostgreSQL

6.1.6 Almacenamiento

Como almacenamiento principal de repositorio de datos se encuentra Google Cloud SQL. Este provee el aprovisionamiento de hardware, configuración, respaldos, actualizaciones y alta disponibilidad.

Como motor de base de datos tenemos a PostgreSQL con Google Cloud Enterprise Plus con las siguientes características:

- ANS de disponibilidad: 99.99%
- Tipo de máquina: Familia de N optimizada para el rendimiento
- Límites de configuración de máquinas: Hasta 128 CPU virtuales, Hasta 864 GB de RAM

6.1.7 Sistema de respaldos y conservación de información

Cada servicio tiene su propio sistema de respaldos. Estos respaldos son absolutos, lo cual provee de un respaldo completo de todos los datos desde el inicio de las operaciones de la CA. Los plazos de conservación de la información, de conformidad con la finalidad del tratamiento que realizará la CA, será de dos años para información de certificados de una vigencia menor a dos años y para certificados con una vigencia igual o mayor a dos años será por el tiempo de duración del certificado más dos meses, por ejemplo si un certificado tiene vigencia de 1 mes se conservarán sus registros por 2 años, y si el certificado tiene vigencia de 5 años se conservarán sus registros por 5 años y 2 meses.

Dicha conservación se realiza con la única finalidad de respetar la normativa vigente y las obligaciones que pueda tener la CA de entregar o conservar información, de conformidad con su política de privacidad y la

normativa vigente.

Respaldo de base de datos:

Los respaldos de la base de datos son gestionados automáticamente por el servicio de Google Cloud SQL. Estos son persistidos de forma multirregional en el centro de datos de Estados Unidos con una retención de 7 días y frecuencia diaria entre las 01:00 y 05:00 (UTC-5) horas.

En caso de requerir un backup en un momento específico un usuario con rol Operador de Respaldos puede solicitar un backup y exportarlo hacia Google cloud storage.

Google Kubernetes Engine:

Por medio del servicio de "Copia de seguridad para GKE" propio de GCP se obtiene un respaldo completo de las configuraciones, cargas de trabajo y recursos del clúster privado desplegado.

Este respaldo se almacena en us-east4 (Virginia del Norte) con una política de retención de 7 días y una frecuencia de ejecución diaria a las 01H00 (UTC-5) horas.

6.1.8 Red san

No se utiliza una red de área de almacenamiento.

6.1.9 Data center

Los centros de datos son completamente administrados por GCP, estos se encuentran en diferentes regiones del mundo.

FIRMASEGURA S.A.S opta por el centro de datos en Carolina del Sur (us-east1) el cual brinda una menor latencia con Ecuador

6.1.10 Seguridad

Acceso a GCP y AWS:

- Usuarios asignados por el administrador que cuenten con cuenta de correo empresarial con doble factor de autenticación.
- Asignación de roles y privilegios específicos a las funciones a realizar de cada usuario por parte del administrador.

6.1.11 Detalle de hardware y software y diagrama esquemático y descripción técnica detallada de la infraestructura a ser utilizada, indicando las características técnicas de la misma

El hardware utilizado en la CA se encuentra detallado en la sección 6.1.5 Servidores.

El diagrama esquemático se encuentra detallado en la sección: 6.1.1 Descripción del esquema de red

El software para el funcionamiento de la infraestructura es brindado por servicios de GCP. El software que brinda los servicios de red se encuentra en la sección 6.1.1 Descripción del esquema de red.

Por otra parte, los servicios complementarios son:

6.1.11.1Google Kubernetes Engine (GKE)

Servicio de Kubernetes basado en la nube fácil de usar para ejecutar aplicaciones en contenedores.

6.1.11.2Google Cloud Logging

Servicio de gestión de registros totalmente gestionada y en tiempo real, que admite exabytes de datos y ofrece funciones de almacenamiento, búsqueda, análisis y alertas.

6.1.11.3Google Cloud Monitoring

Recopila mediciones de servicios y recursos de Google Cloud Platform.

6.1.11.4Google Cloud SQL

Es un servicio de bases de datos completamente administrado que ayuda a configurar, mantener y administrar las bases de datos relacionales en Google Cloud Platform.

6.1.11.5Google Cloud Storage

Servicio para almacenar objetos en Google Cloud. Un objeto es un dato inmutable que consta de un archivo de cualquier formato. Los objetos se almacenan en contenedores llamados buckets.

6.1.11.6Amazon Private CA

Autoridad de certificación privada de AWS permite la creación de jerarquías de entidades de certificación (CA) privadas, incluidas las entidades de certificación raíz y subordinadas

6.1.12 Ubicación y distribución de equipos

Los servicios se encuentran desplegados en Moncks Corner, Carolina del Sur, Norteamérica (us-east1).

La distribución de equipos en racks es gestionada por Google Cloud Platform.

6.1.13 Esquema de conectividad

Se establecen 2 formas para conectarse a la plataforma que dependerá del tipo de usuario:

6.1.13.1Acceso a usuarios

Son las personas que requieren solicitar un certificado electrónico. Este tipo de usuarios solo pueden tener acceso al portal público de FIRMASEGURA S.A.S y a los servicios de CRL y OCSP.

También existen usuarios que son empleados registrados y validados por FIRMASEGURA S.A.S que actuarán como verificadores de información de las personas solicitantes.

6.1.13.2Acceso a administradores de la infraestructura

Los administradores de infraestructura son encargados de realizar seguimiento al funcionamiento de los servicios y monitoreo de los mismos. También realizan cambios de escalamiento en servicios a través de las consolas de administración de Google Cloud Platform.

Los empleados asignados, tienen un contrato de confidencialidad de la información con la compañía, asegurando así la idoneidad y seguridad de los mismos para acceder a la infraestructura.

El control de acceso para este tipo de usuarios es debidamente administrado desde Google Cloud Platform por parte del administrador principal.

Como parte de la alianza estratégica entre FIRMASEGURA S.A.S. y ALQUIMIASOFT S.A. se establece que personal de ALQUIMIASOFT podrá brindar servicios, basados en su experiencia, relacionados con Arquitectura, Infraestructura y programación a FIRMASEGURA S.A.S., y deberán cumplir con estrictos

procesos de control para brindar estos servicios.

6.1.14 Topología de conectividad

La topología física es completamente administrada por Google Cloud Platform. Los accesos para su gestión lógica se establecen por medio de la consola de administración.

6.1.15 Esquema de cómputo

Los servicios desplegados sobre la plataforma están diseñados para brindar una alta disponibilidad. Estos servicios se pueden revisar en la sección: 6.1.11 Detalle de hardware y software.

6.1.16 Hardware criptográfico HSM

FIRMASEGURA S.A.S utiliza AWS Private CA que cuenta con módulo de seguridad de hardware (HSM) gestionados por AWS con estándar de seguridad certificado FIPS 140-2 nivel 3 con el fin de alojar claves de encriptación y realizar operaciones criptográficas.

6.1.17 Esquema de respaldos

Se utilizan respaldos automáticos proveídos por los servicios de Google Cloud Platform.

Los sistemas de respaldos se establecen en la sección: 6.1.7 Sistema de respaldos.

6.2 Sitio seguro secundario

Para brindar alta disponibilidad se distribuyen en zonas los sitios seguros. Por lo tanto la infraestructura implementada es la misma y solo se distribuyen por configuración.

6.2.1 Descripción del esquema de red

Ver la sección 6.1.1 Descripción del esquema de red

6.2.1.1 Dispositivos de seguridad de borde

Ver la sección 6.1.1 Dispositivos de seguridad de borde.

6.2.2 Almacenamiento

Ver la sección 6.1.6 Almacenamiento.

6.2.3 Red de comunicaciones

Ver la sección 6.1.4 Conectividad LAN.

7 Ubicación geográfica de cada nodo o sitio seguro

7.1 Sitio principal

El centro de datos está ubicado en la región de us-east1 de GCP, en la ciudad de Moncks Corner, Carolina del Sur, Estados Unidos.

Esta región cuenta con tres zonas. Se utiliza la zona B preferentemente.

7.2 Sitio alterno

El centro de datos está ubicado en la región de us-east1 de GCP, en la ciudad de Moncks Corner, Carolina

del Sur, Estados Unidos.

Esta región cuenta con tres zonas. Se utiliza la zona C preferentemente o cualquier zona diferente a la principal.

8 Documentos de soporte que confirman que se dispone de mecanismos de seguridad

8.1 Mecanismos de seguridad

FIRMASEGURA S.A.S. cuenta con políticas y procedimientos específicos para la generación y protección de claves criptográficas, que se llevan a cabo en un ambiente controlado y seguro, con acceso limitado y restringido a personal autorizado, el personal autorizado y el procedimiento para su acceso.

Se cuenta con sistemas de resguardo y protección contra siniestros para los documentos y equipos involucrados en los procesos de certificación, tales como sistemas de alimentación ininterrumpida (UPS) y sistemas de respaldo de información.

Se implementan controles de acceso físico y lógico para proteger los sistemas y la información contra posibles ataques, intrusiones o amenazas.

Además, se establecen procedimientos para la verificación y autenticidad de los certificados, de manera que se evita la falsificación o manipulación de la información.

Descripción de sistemas de seguridad, estándares de seguridad y sistemas de respaldo

FIRMASEGURA S.A.S. implementa sistemas y controles de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información, siguiendo los estándares y mejores prácticas de la industria.

Los sistemas de seguridad incluyen sistemas de detección y prevención de intrusiones, sistemas de protección de la red, sistemas de monitoreo y auditoría, y sistemas de encriptación de la información.

Además, se establecen políticas y procedimientos para la realización de respaldos de información conforme se detalla en el acápite 8.16, del Plan de Contingencia acápite 8.9 y del Plan de Recuperación ante desastres acápite 8.11, para garantizar la seguridad e integridad de la información.

Procedimientos para la protección de los datos personales de los solicitantes y usuarios de los servicios de certificación:

FIRMASEGURA S.A.S. cumple con las leyes y regulaciones aplicables en materia de privacidad y protección de datos personales.

Se establecen procedimientos específicos para la recopilación, procesamiento y almacenamiento de datos personales de los solicitantes y usuarios, garantizando su confidencialidad y seguridad conforme se detalla en el numeral 8.5.6 del presente documento.

Se implementan controles de acceso y autenticación para la gestión y acceso a los datos personales, y se establecen procedimientos para la eliminación segura de los datos personales de los solicitantes y usuarios, una vez que se haya cumplido con el plazo de retención establecido por la ley, conforme se detalla en el numeral 8.5 de esta DPC.

Medidas de Seguridad Lógica:

Control de Acceso: Se gestionan los accesos lógicos a sistemas y datos críticos. Se implementan políticas

de acceso basadas en roles.

Encriptación de Datos: Se utiliza la encriptación para proteger la confidencialidad de los datos almacenados y transmitidos. Incluye la encriptación de las claves privadas de los certificados y la comunicación segura entre la CA y los solicitantes.

Monitoreo y Detección de Intrusiones: Implementación de herramientas para monitorear y detectar actividades inusuales o maliciosas en la infraestructura de la CA. Se incluyen sistemas de detección de intrusiones y registros de auditoría.

Auditorías y Revisiones: Se realizan auditorías de seguridad al menos una vez al año para evaluar el cumplimiento de políticas y procedimientos.

Medidas de Seguridad Física:

Seguridad de las Instalaciones: Al utilizar los servicios bajo demanda de Google Cloud Platform incorpora múltiples capas de seguridad física. El acceso a estos centros de datos está muy controlado. GCP utiliza múltiples capas de seguridad física para proteger los pisos de nuestro centro de datos. GCP utiliza identificación biométrica, detección de metales, cámaras, barreras para vehículos y sistemas de detección de intrusiones.

Respaldo y Almacenamiento de Medios: Se realizan los respaldos de datos críticos y se almacenan de manera segura los medios de respaldo para la recuperación en caso de fallo o pérdida de datos, conforme la Política de Respaldo establecida en el acápite 8.16 de la DPC.

Eliminación Segura de Medios y Hardware: Se establece el procedimiento para la eliminación segura de hardware y medios de almacenamiento que ya no se utilizan, para evitar la exposición de información confidencial conforme se detalla en el acápite 8.5.

8.1.1 Seguridad a través de la criptografía

La criptografía desempeña un papel fundamental en la seguridad de la información y la privacidad de los mensajes transmitidos en el entorno digital. A través de la aplicación de algoritmos criptográficos, se protege la confidencialidad, la integridad y la autenticidad de los datos, lo que garantiza que solo las partes autorizadas tengan acceso a la información y que esta no sea modificada durante su transmisión.

Llaves Criptográficas Simétricas y Asimétricas:

Existen dos enfoques clave en criptografía: simétrica y asimétrica. La criptografía simétrica implica el uso de una única llave para cifrar y descifrar datos. Ambas partes que se comunican deben conocer esta llave compartida, lo que puede plantear desafíos en términos de distribución segura de la llave.

Por otro lado, la criptografía asimétrica utiliza un par de llaves: una pública y una privada. La llave pública es de conocimiento público y está disponible para cualquier entidad que quiera comunicarse con el titular de la llave privada. En cambio, la llave privada se mantiene en secreto y solo el titular puede acceder a ella. Este enfoque se conoce como criptografía de llave pública y privada.

Funcionamiento de la Criptografía de Llave Pública y Privada:

En el contexto de la criptografía de llave pública y privada, la llave privada se utiliza para firmar los mensajes. Cuando un remitente firma un mensaje con su llave privada, se genera una firma de firma electrónica única que autentica la fuente del mensaje. Esta firma de firma electrónica es verificable

utilizando la llave pública correspondiente. La llave pública se utiliza para verificar la firma, y su disponibilidad pública permite que cualquier entidad pueda realizar esta verificación.

Ventajas de la Criptografía de Llave Pública y Privada:

Una de las principales ventajas de la criptografía de llave pública y privada es la libre distribución de las llaves públicas. Como estas llaves son de conocimiento público y no representan un riesgo de seguridad si se revelan, pueden distribuirse ampliamente y utilizarse para verificar firmas electrónicas, autenticar remitentes y establecer comunicaciones seguras.

Además, la criptografía de llave pública y privada permite una comunicación segura incluso en un entorno donde las partes no se conocen previamente, ya que pueden verificar la autenticidad de los mensajes sin la necesidad de compartir una llave común de cifrado.

8.1.2 Certificado de firma electrónica

El certificado de firma electrónica es una pieza fundamental en el mundo de la seguridad digital. Se crea a partir de la llave privada generada por el sistema y tiene un propósito clave: garantizar la identidad de una persona o entidad en el entorno digital y permitir la firma electrónica de documentos. A través de un certificado de firma electrónica, se establece un vínculo sólido entre una identidad en línea y la llave privada correspondiente.

Autenticidad y Confianza:

Cuando alguien recibe un documento firmado electrónicamente, puede confiar en su autenticidad. El certificado de firma electrónica asegura que el documento es el original y que no ha sido manipulado en el proceso de envío. Esto se logra mediante la firma electrónica, que actúa como un sello de garantía. Quien firma el documento no puede negar la autoría de la firma, lo que se conoce como "no repudio". Esta característica es esencial en transacciones electrónicas, contratos y comunicaciones críticas.

Contenido del Certificado de firma electrónica:

El certificado de firma electrónica contiene información clave. En primer lugar, incluye la llave pública correspondiente al titular del certificado. Esta llave pública es esencial para la verificación de las firmas electrónicas realizadas por el titular. Además, el certificado de firma electrónica contiene información sobre el titular, que puede incluir su nombre, dirección de correo electrónico, entidad a la que representa y otros datos relevantes.

Firma de la Entidad de Certificación (CA):

Un componente esencial del certificado de firma electrónica es la firma de la entidad de certificación, también conocida como Autoridad de Certificación (CA). La CA es una entidad de confianza que verifica la identidad del titular del certificado y garantiza que los datos del titular son correspondientes con la llave pública. La firma de la CA es un sello de autenticación que valida la legitimidad del certificado de firma electrónica.

8.1.3 Entidad de certificación

Autoridad de certificación privada de AWS permite la creación de jerarquías de entidades de certificación (CA) privadas, incluidas las entidades de certificación raíz y subordinadas. Las entidades de certificación privadas pueden emitir certificados X.509 de entidad final útiles en situaciones tales como certificados para firma electrónica.

Autoridad de Certificación (CA) en AWS Private CA:

Aspectos clave de la entidad de certificación ofrecida por AWS Private CA:

Emisión de Certificados de firma electrónica:

AWS Private CA permite la emisión de una amplia gama de certificados de firma electrónica, incluidos firma electrónica, cifrado y autenticación.

Cumplimiento de Normativas:

AWS Private CA se adhiere a estándares y regulaciones de seguridad, incluidos los requisitos de cumplimiento normativo, lo que lo hace adecuado para entornos altamente regulados.

Escalabilidad:

AWS Private CA es escalable y se adapta a las necesidades de diferentes organizaciones, desde pequeñas empresas hasta grandes empresas y gobiernos.

Interoperabilidad:

AWS Private CA es compatible con una variedad de protocolos y estándares de la industria, lo que facilita su integración en entornos de TI existentes.

Administración de Ciclo de Vida de Certificados:

AWS Private CA permite la gestión completa del ciclo de vida de los certificados, lo que incluye emisión, renovación, revocación y caducidad.

Autenticación y Firma Electrónica:

AWS Private CA admite la autenticación de usuarios mediante certificados de firma electrónica, lo que garantiza la seguridad en las comunicaciones y transacciones en línea.

Seguridad de Claves:

AWS Private CA proporciona una sólida seguridad para las claves privadas utilizadas en la emisión de certificados, lo que protege contra amenazas y ataques.
Las claves privadas de las CA privadas se almacenan en módulos de seguridad de hardware (HSM) AWS gestionados. Los HSM cumplen con los requisitos de seguridad FIPS PUB 140-2 de nivel 3 para los módulos criptográficos.

Auditoría y Registro:

AWS Private CA registra todas las operaciones críticas y permite la realización de auditorías para garantizar la conformidad y la seguridad.

Soporte de Cifrado y Firmas Fuertes:

AWS Private CA utiliza algoritmos de cifrado y firmas robustas para garantizar la seguridad de los certificados de firma electrónica emitidos.

8.1.4 Algoritmos

Algoritmo RSA: Seguridad Asimétrica en la Comunicación

El algoritmo RSA, denominado por las iniciales de sus creadores, Rivest, Shamir y Adleman, es un

algoritmo de cifrado de clave pública ampliamente utilizado en la criptografía moderna. Se basa en un par de claves asimétricas: una llave pública y una llave privada. La llave pública se utiliza para cifrar mensajes, mientras que la llave privada se emplea para descifrarlos. Esto permite que las partes que se comunican compartan información de manera segura sin necesidad de compartir una llave secreta común.

El algoritmo RSA se basa en la factorización de números enteros en sus factores primos. Al generar un par de claves RSA, se eligen dos números primos grandes, cada uno con más de 100 dígitos. Estos números primos se mantienen en secreto y se utilizan para calcular la clave privada. La seguridad del algoritmo RSA radica en la dificultad de factorizar números enteros grandes en sus factores primos. Hasta la fecha, no existe un método rápido para factorizar números tan grandes, lo que hace que el algoritmo RSA sea altamente seguro.

Este algoritmo es ampliamente utilizado en aplicaciones que requieren comunicaciones seguras, como SSL/TLS para la protección de sitios web, correo electrónico seguro y firmas electrónicas. Para obtener más detalles técnicos sobre el algoritmo RSA, se puede consultar la página: https://datatracker.ietf.org/doc/html/rfc8017

Algoritmo SHA: Integridad y Verificación en la Criptografía

El algoritmo SHA, que significa "Secure Hash Algorithm" (Algoritmo de Hash Seguro), es una función hash criptográfica ampliamente adoptada que produce una salida de 256 bits. A diferencia de los algoritmos de cifrado que utilizan claves, el algoritmo SHA es una función de resumen que no requiere una llave para su funcionamiento. Su principal propósito es garantizar la integridad de los datos y detectar cualquier manipulación o cambios no autorizados en la información transmitida.

Cuando se aplica el algoritmo SHA a un conjunto de datos, se genera un valor único llamado hash. Este hash es una representación fija y compacta de los datos originales. Incluso un pequeño cambio en los datos originales resultará en un hash completamente diferente. Esto permite verificar si los datos han sido alterados durante la transmisión, lo que garantiza su inmutabilidad.

El algoritmo SHA se utiliza en combinación con certificados de firma electrónica para proteger la integridad de los datos que se envían y reciben. La firma de un mensaje con un certificado de firma electrónica y el uso del algoritmo SHA para calcular el hash del mensaje garantizan que los datos no se han alterado y que provienen de la fuente autenticada.

Para obtener más información técnica sobre el algoritmo SHA, puedes consultar la página: https://datatracker.ietf.org/doc/html/rfc4634

8.2 Contenedores criptográficos

En el ámbito de la seguridad de la información, los contenedores criptográficos desempeñan un papel esencial al proporcionar un espacio seguro para el almacenamiento y la gestión de llaves privadas y certificados de firma electrónica. Uno de los contenedores criptográficos más utilizados en sistemas es el Almacén de Llaves (Keystore en inglés).

Almacén de Llaves (Keystore):

El Almacén de Llaves es un contenedor seguro diseñado para guardar llaves privadas y certificados de firma electrónica. En el contexto de sistemas que utilizan certificados de firma electrónica, los titulares de certificados descargan este contenedor en forma de archivo para almacenar sus claves privadas y

certificados de manera segura.

Formato PKCS#12 y Proceso de Certificación:

Dentro del Almacén de Llaves, se guarda el certificado de firma electrónica, que utiliza el formato PKCS#12. Este formato se caracteriza por contener un certificado que ya ha sido firmado por la Autoridad de Certificación (AC). Inicialmente, el proceso comienza con la creación de un contenedor en formato PKCS#12, que es una solicitud de firma de certificado (CSR). Esta solicitud es enviada a la AC para su aprobación.

La AC revisa la solicitud y, una vez aprobada, emite un certificado de firma electrónica. Este certificado de firma electrónica permite a su titular realizar una serie de acciones seguras en línea, como firmar documentos electrónicos, autenticarse en servicios web y proteger la confidencialidad de las comunicaciones.

8.3 Especificaciones técnicas de los contenedores

En el contexto de nuestra infraestructura de certificación, un contenedor criptográfico es un archivo que almacena claves privadas, certificados de firma electrónica y otros datos sensibles de forma segura. Estos contenedores actúan como cajas fuertes virtuales para proteger la información crítica.

Tipos de Contenedores Utilizados: Nuestra infraestructura utiliza principalmente contenedores en formato PKCS#12 (.p12) para almacenar claves privadas y certificados de firma electrónica. Estos contenedores son compatibles con una amplia gama de aplicaciones y sistemas.

Formato de Contenedores: Los contenedores PKCS#12 utilizados tienen un formato de archivo binario que incluye tanto claves privadas como certificados de firma electrónica. Este formato es ampliamente reconocido y es compatible con numerosas aplicaciones y sistemas.

Normas y Estándares de Contenedores: Nuestros contenedores cumplen con las normas PKCS#12 y X.509, que establecen estándares ampliamente aceptados en la industria para la gestión de claves privadas y certificados digitales. Además, se siguen las mejores prácticas de seguridad de AWS Private CA y GCP.

8.4 Estándares y normas internacionales

8.4.1 Normas, estándares

8.4.1.1 Leyes y regulaciones aplicables

FIRMASEGURA S.A.S se rige por las leyes y regulaciones aplicables en la República del Ecuador, incluyendo, entre otras, la Constitución de la República del Ecuador, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, y su Reglamento, la Ley de Protección de Datos Personales, las normas y regulaciones emitidas por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) y cualquier otra normativa relacionada con la seguridad de la información y la privacidad de los datos personales.

8.4.1.2 Políticas y estándares relacionados

FIRMASEGURA S.A.S seguirá las políticas y estándares relacionados con la seguridad de la información y la privacidad de los datos personales, incluyendo los estándares establecidos por la International Organization for Standardization (ISO) en las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013. Además, FIRMASEGURA S.A.S seguirá las políticas y estándares establecidos por el RFC 3647 "Internet

X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

La RFC 3647, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" (Marco de Política de Certificados e Implementación de Prácticas de Certificación de Infraestructura de Clave Pública X.509 en Internet)

Es un estándar desarrollado por la Internet Engineering Task Force (IETF) que se centra en la creación de políticas y prácticas para la emisión y gestión de certificados digitales en Internet. Esta norma proporciona directrices y un marco para establecer políticas y prácticas de certificación de clave pública en entornos de Internet, y es fundamental para garantizar la interoperabilidad y la seguridad de las infraestructuras de clave pública (PKI) en línea.

La RFC 3647 establece un marco que las Autoridades de Certificación (AC) y otras partes interesadas deben seguir al definir políticas y prácticas de certificación de clave pública en Internet.

Proporciona un enfoque estructurado y coherente para garantizar la seguridad y la confianza en los certificados de firma electrónica emitidos y utilizados en línea.

Define la necesidad de establecer políticas de certificación que rigen la emisión y gestión de certificados de firma electrónica. Las políticas de certificación describen los procedimientos y requisitos que deben cumplirse para emitir y gestionar certificados de firma electrónica.

La RFC 3647 sugiere que las políticas de certificación deben incluir información sobre la identificación de solicitantes, los procedimientos de verificación, los tiempos de validez de los certificados y los métodos de revocación, entre otros aspectos.

Define la necesidad de establecer prácticas de certificación que detallen cómo se implementan las políticas de certificación en la práctica.

Las prácticas de certificación describen los procedimientos específicos que una Autoridad de Certificación (CA) sigue para emitir, renovar y revocar certificados de firma electrónica.

La RFC 3647 aborda la importancia de establecer relaciones de confianza entre CAs y con otras partes interesadas en el ecosistema de certificados de firma electrónica en Internet.

La RFC 3647 menciona que las CAs deben emitir certificados de firma electrónica en conformidad con la versión 3 del estándar X.509, que es la versión más utilizada y versátil.

La norma destaca la importancia de usar extensiones en los certificados de firma electrónica para proporcionar información adicional. Entre las extensiones comunes se incluyen KeyUsage, AuthorityKeyIdentifier y Certificate Policies.

La RFC 3647 es esencial para garantizar la seguridad y la confianza en la emisión y gestión de certificados de firma electrónica en Internet. Al seguir este marco, las organizaciones pueden establecer políticas y prácticas sólidas que cumplen con los estándares de la industria y garantizan la interoperabilidad en el entorno en línea.

Norma ISO/IEC 9594-8 y Estándar X.509 en Certificados de firma electrónica:

La norma ISO/IEC 9594-8 y el estándar X.509 son fundamentales para garantizar la interoperabilidad y la seguridad de los certificados de firma electrónica. Estas normas establecen los requisitos técnicos y los campos obligatorios que deben incluirse en un certificado de firma electrónica.

Campos Obligatorios en un Certificado de firma electrónica:

Un certificado de firma electrónica debe contener ciertos campos obligatorios para garantizar su validez y autenticidad. Estos campos incluyen:

Datos del Certificado:

Versión: Indica la versión del estándar X.509 que se está utilizando en el certificado.

Número de serie: Un número único que identifica de manera única el certificado.

Emisor del Certificado: La entidad que emite el certificado, generalmente una Autoridad de Certificación (AC).

Validez: Incluye la fecha de inicio y la fecha final de validez del certificado.

Nombre Distinguido del Sujeto: La entidad o persona a la que se otorga el certificado.

Llave Pública del Sujeto: La clave pública correspondiente al titular del certificado.

Firma del Certificado:

Algoritmo de Firma: El algoritmo criptográfico utilizado para firmar el certificado.

Firma del Certificado: La firma electrónica generada con la clave privada del emisor para autenticar el certificado.

Extensiones en un Certificado de firma electrónica:

Además de los campos obligatorios, los certificados de firma electrónica pueden incluir extensiones que proporcionan información adicional o detalles sobre su uso. Las extensiones comunes incluyen:

KeyUsage (Uso de Clave):

Especifica los posibles usos del certificado. En el contexto de firma electrónica de documentos, comúnmente se utiliza el valor "DigitalSignature" para indicar que el certificado se emplea para firmar documentos electrónicos.

AuthorityKeyIdentifier (Identificador de Clave de Autoridad):

Esta extensión identifica un certificado de clave pública de la Autoridad de Certificación (AC) asociado con la llave privada utilizada para firmar el certificado. Ayuda a establecer la relación entre el certificado y la AC que lo emitió.

Certificate Policies (Políticas de Certificación):

Esta extensión específica la política de certificación que la AC sigue al emitir certificados. Define las prácticas y los estándares que rigen la emisión y el uso de los certificados.

Es importante destacar que los certificados de firma electrónica cumplen con la versión 3 del estándar X.509, que es la más ampliamente utilizada y proporciona la flexibilidad necesaria para acomodar diversas aplicaciones de seguridad digital. Estos estándares son esenciales para garantizar la coherencia y la confiabilidad en la implementación de certificados de firma electrónica en sistemas y servicios que requieren autenticación y seguridad en línea.

RFC 2560 - OCSP: Protocolo de Estado de Certificado en Línea

El Protocolo de Estado de Certificado en Línea (OCSP) es una tecnología que permite cumplir con los requisitos operativos relacionados con la información de revocación de certificados digitales de una manera más ágil y oportuna que la Lista de Revocación de Certificados (CRL). OCSP se basa en la norma RFC 2560 y es una parte fundamental de la infraestructura de clave pública (PKI) de Internet.

Respuestas OCSP:

Las respuestas OCSP son la forma en que los solicitantes obtienen información sobre el estado de un certificado de firma electrónica en un momento dado. Estas respuestas se generan de acuerdo con la versión 0 (equivalente a la versión 1) por defecto. Sin embargo, OCSP puede incluir extensiones para funciones adicionales:

Nonce (Número Aleatorio): Esta extensión permite vincular de forma criptográfica una solicitud y una respuesta, garantizando la integridad de la comunicación.

CRL References (Referencias de Lista de Revocación de Certificados):

Esta extensión indica la ubicación de la CRL que contiene información sobre certificados revocados. Ayuda en el proceso de auditoría y se identifica mediante el objeto id-pkix-ocsp-crl.

Datos de Solicitud OCSP (OCSP Request):

Una solicitud OCSP consta de los siguientes elementos de acuerdo con la norma RFC 2560:

Versión de Protocolo: Indica la versión del protocolo OCSP utilizada.

Solicitud de Servicio: Especifica el tipo de servicio que se solicita, como la verificación del estado de un certificado.

Identificador del Certificado Objetivo: Es el certificado del que se desea verificar el estado.

Extensiones Opcionales: Pueden incluirse para requisitos o funciones específicas.

Proceso de Respuesta OCSP:

Cuando un servidor OCSP recibe una solicitud, realiza varias verificaciones. Estas verificaciones incluyen:

Verificación de la estructura de la solicitud.

Confirmación de que el servidor está configurado para proporcionar el servicio solicitado.

Aseguramiento de que la solicitud contiene la información requerida.

Si alguna de estas condiciones falla, el servidor OCSP produce un mensaje de error en respuesta.

Componentes de una Respuesta OCSP:

Una respuesta OCSP está compuesta por varios componentes esenciales:

Versión de la Sintaxis de Respuesta: Indica la versión del formato de respuesta OCSP.

Nombre de Quien Responde: El identificador del servidor que emite la respuesta.

Respuestas para Cada Certificado en la Solicitud: Para cada certificado en la solicitud, se proporciona información sobre su estado de validez.

Extensiones Opcionales: Se incluyen para funciones o requisitos específicos.

Algoritmo de Firma OID: El algoritmo criptográfico utilizado para firmar la respuesta.

Firma Computada Utilizando el Hash de la Respuesta: La firma electrónica que autentica la respuesta OCSP.

Respuesta para Cada Certificado:

La respuesta para cada certificado en una solicitud contiene detalles importantes:

Identificador del Certificado Objetivo: Identifica el certificado que se verifica.

Estado del Certificado: Indica si el certificado está vigente, revocado u otro estado.

Intervalo de Validez de la Respuesta: Establece el período de validez de la respuesta OCSP.

Extensiones Opcionales: Pueden incluirse extensiones adicionales para cumplir con requisitos específicos.

8.4.1.3 Contratos y acuerdos

FIRMASEGURA S.A.S establecerá un contrato con sus clientes para la prestación de servicios de firma electrónica en archivo .p12 en los que se establecerán las responsabilidades y obligaciones de ambas partes, incluyendo los términos y condiciones de uso de los certificados, las políticas de renovación, revocación y suspensión de certificados, y cualquier otra cláusula necesaria para garantizar la seguridad y privacidad de la información y los datos personales. Dichos contratos serán aceptados por el usuario al momento de aceptar los términos y condiciones de la firma electrónica y contienen disposiciones de conformidad con la Ley Orgánica de Defensa al Consumidor y demás normativa aplicable.

8.4.1.4 Requerimientos de privacidad y protección de datos personales

FIRMASEGURA S.A.S garantizará la privacidad y protección de los datos personales de sus clientes, siguiendo los requerimientos establecidos en la Ley de Protección de Datos Personales y cualquier otra normativa relacionada. Los datos personales de los clientes serán tratados de forma confidencial y sólo serán utilizados para la prestación de los servicios de firma electrónica en archivo .p12, Además, FIRMASEGURA S.A.S implementará las medidas de seguridad necesarias para garantizar la protección de los datos personales de sus clientes, incluyendo medidas técnicas y organizativas para prevenir el acceso no autorizado, la divulgación y cualquier otro uso indebido de los datos personales.

8.5 Políticas de Acceso, Gestión de claves, Auditoría, Control de cambios, Mejora continua y Protección de datos personales, y mecanismos de seguridad para evitar la falsificación de certificados, precautelar la integridad, resguardo de documentos, protección contra siniestros, control de acceso y confidencialidad durante la generación de claves

8.5.1 FIRMASEGURA S.A.S. cuenta con políticas y procedimientos específicos para el acceso y autenticación a su infraestructura, para la generación y protección de claves criptográficas, para Auditoría y monitoreo permanente, para la gestión de cambios que garanticen su disponibilidad, para el cumplimiento y mejora continua de sus políticas y para asegurar la confidencialidad y protección de datos personales, las mismas que se detallan a continuación: Políticas de Acceso y Autenticación:

Se establece la política de acceso estricto para el HSM. Solo usuarios y sistemas autorizados deben tener acceso al HSM. En este caso solamente los Roles de Administradores de HSM, Operadores de HSM y Respuesta a Incidentes.

Roles de Personal Autorizado para Acceder al HSM:

Administradores de HSM: Estos son responsables de la gestión, configuración y control de acceso al HSM. Sus roles y responsabilidades incluyen:

Aprobar solicitudes de acceso al HSM.

Configurar y mantener el HSM.

Realizar auditorías y supervisar el cumplimiento de la política de acceso al HSM.

Mantener registros de acceso y auditoría relacionados con el HSM.

Operadores del HSM: Este personal está autorizado para llevar a cabo operaciones directas en el HSM, como la generación de claves y certificados, y para realizar operaciones de respaldo y recuperación. Sus roles y responsabilidades incluyen:

Generar y administrar claves y certificados en el HSM.

Mantener registros detallados de las operaciones realizadas en el HSM.

Personal de Respuesta a Incidentes: Este personal tiene acceso al HSM en situaciones de respuesta a incidentes de seguridad o de recuperación de desastres. Sus roles y responsabilidades incluyen:

Evaluar la necesidad de acceso al HSM en situaciones de incidentes de seguridad o recuperación.

Motivos para Acceso Autorizado al HSM:

El personal autorizado puede acceder al HSM en los siguientes casos:

Operaciones de Administración Regular: Los administradores de HSM y operadores del HSM tienen acceso para llevar a cabo operaciones regulares de administración, como la generación y gestión de claves y certificados.

Operaciones de Respuesta a Incidentes: El personal de respuesta a incidentes puede acceder al HSM en situaciones de respuesta a incidentes de seguridad o recuperación de desastres para garantizar la continuidad de las operaciones de la CA.

Procedimiento para Control de Acceso Autorizado al HSM:

Solicitud de Acceso: Cualquier solicitud de acceso al HSM debe ser presentada por el personal autorizado a los administradores de HSM. La solicitud debe incluir una justificación válida y detalles sobre el motivo del acceso.

Evaluación y Aprobación: El personal de seguridad de la CA evaluará y aprobará la solicitud de acceso al HSM. Esto incluirá verificar que la solicitud esté respaldada por motivos legítimos y que el solicitante esté debidamente autenticado.

Realización de la Operación: Una vez aprobada, la operación de acceso autorizado al HSM se llevará a cabo de acuerdo con los procedimientos establecidos. Se mantendrán registros detallados de la operación.

Auditoría y Registro: Cada acceso autorizado al HSM se registrará y se mantendrá un registro detallado, incluyendo la fecha, la hora, el motivo y el personal involucrado en la operación.

Monitoreo Continuo:

Se implementa un sistema de monitoreo continuo para detectar cualquier intento no autorizado de acceder

al HSM o cualquier actividad inusual que incluya lo siguiente:

Registro de Acceso:

Se lleva un registro detallado de todas las acciones realizadas en el HSM, incluyendo quién accedió, cuándo y qué operaciones se realizaron.

Actualizaciones y Parches:

Se deberá mantener el firmware y el software del HSM actualizados con los últimos parches de seguridad para protegerlo contra vulnerabilidades conocidas.

8.5.2 Gestión de Ciclo de Vida de las Claves:

Se establece la política para el ciclo de vida de las claves, incluyendo la generación, rotación y eliminación segura de claves privadas cuando sea necesario, conforme se detalla a continuación:

Generación Segura de Claves Privadas:

a. Todas las claves privadas se generarán utilizando métodos de generación criptográfica seguros y aleatorios.

b. Las claves privadas se generarán en un entorno de alta seguridad y en un proceso que garantice la confidencialidad de las mismas.

c. Las claves privadas recién generadas se protegerán inmediatamente y se almacenarán de forma segura.

Rotación Periódica de Claves Privadas:

a. Se implementará un programa de rotación de claves que defina la frecuencia con la que las claves privadas deben ser cambiadas.

b. Antes de la rotación, se generará una nueva clave privada siguiendo los mismos estándares de seguridad que la generación inicial.

c. La nueva clave privada se utilizará para firmar certificados emitidos y se certificará mediante la clave privada anterior.

d. Una vez que se ha certificado la nueva clave privada y se ha actualizado el almacenamiento de claves, la clave privada anterior se revocará y se eliminará de manera segura.

Eliminación Segura de Claves Privadas:

a. Cuando una clave privada se considere obsoleta o haya alcanzado el final de su vida útil, se llevará a cabo un proceso de eliminación segura.

b. La eliminación segura implicará la destrucción de la clave privada en todos los dispositivos de almacenamiento.

c. Se mantendrán registros de la eliminación segura, incluyendo la fecha, la razón y el método utilizado.

Respaldo de Claves Privadas:

a. Se realizarán copias de seguridad regulares de las claves privadas en ubicaciones seguras y aisladas para garantizar la recuperación en caso de pérdida o corrupción conforme se detalla en el acápite 8.16.1.

Acceso Autorizado a Claves Privadas:

a. Solo el personal autorizado tendrá acceso a las claves privadas y su gestión. Conforme se detalla en el acápite 8.5.1 en el cual se establecen además procedimientos para controlar y auditar el acceso a las claves privadas.

Cumplimiento Legal y Regulatorio:

a. Se garantiza el cumplimiento de los requisitos legales y regulatorios relacionados con la gestión de claves privadas.

Evaluación y Mejora Continua:

a. La CA llevará a cabo una revisión al menos de una vez al año de sus prácticas de gestión de claves privadas para mejorar la eficiencia y la seguridad.

Distribución de Certificados:

Respetar obligatoriamente el proceso para la distribución de certificados de firma electrónica a los titulares autorizados. Esto debe incluir autenticación adecuada y cifrado de datos sensibles.

Respuesta a Incidentes:

El Plan de Respuesta a Incidentes que amenacen a la Seguridad de Claves Privadas se detalla a continuación:

1. Detección de la Amenaza:

La detección de una amenaza a la seguridad de las claves privadas puede ocurrir a través del monitoreo continuo, auditorías de seguridad, alertas de seguridad, registros de actividad inusuales o incidentes reportados por personal o sistemas de detección.

2. Notificación Inmediata:

Cualquier persona que detecte o sospeche una amenaza a la seguridad de las claves privadas deberá notificar de inmediato al equipo de respuesta a incidentes de la CA y a los administradores de seguridad.

3. Evaluación Preliminar:

El equipo de respuesta a incidentes llevará a cabo una evaluación preliminar para determinar la naturaleza y la gravedad de la amenaza.

4. Aislamiento y Contención:

Si es necesario, se tomarán medidas para aislar y contener la amenaza. Esto puede incluir desconectar sistemas comprometidos o desactivar claves privadas afectadas.

5. Análisis de la Amenaza:

Se llevará a cabo un análisis en profundidad de la amenaza, investigando cómo ocurrió y cuál fue su alcance. Esto incluirá un análisis forense de sistemas afectados.

6. Recuperación:

Se implementarán medidas para la recuperación, lo que puede incluir la regeneración de claves privadas comprometidas, la revocación de certificados afectados y la restauración de sistemas a un estado seguro.

7. Comunicación y Notificación:

Se informará a las partes pertinentes, incluyendo a los titulares de certificados afectados, sobre la amenaza y las medidas tomadas.

8. Revisión y Mejora:

Se llevará a cabo una revisión exhaustiva de la amenaza, la respuesta y las medidas tomadas para determinar cómo mejorar la seguridad y prevenir futuros incidentes similares.

9. Cumplimiento Legal y Regulatorio:

Se asegurará el cumplimiento de los requisitos legales y regulatorios relacionados con la notificación de incidentes y la gestión de claves privadas.

10. Capacitación y Concientización:

El personal involucrado será capacitado sobre cómo detectar, notificar y responder a amenazas de seguridad de claves privadas.

11. Documentación y Registro:

Todas las etapas de la respuesta a incidentes, incluyendo la detección, análisis, acciones tomadas y comunicaciones, se documentarán y se mantendrán como registros para futuras referencias.

12. Actualización de Políticas y Procedimientos:

Si es necesario, se actualizarán las políticas y procedimientos de seguridad de la CA para abordar las lecciones aprendidas y prevenir incidentes similares en el futuro.

Capacitación del Personal:

Proporcionar capacitación semestralmente al personal involucrado en la gestión y protección de las claves privadas. Esto incluye la conciencia de seguridad y las mejores prácticas criptográficas.

Auditoría y Cumplimiento:

Realizar auditorías de seguridad para garantizar el cumplimiento de las políticas y procedimientos establecidos y para identificar posibles áreas de mejora, una vez al año por personal especializado en el área.

Revocación y suspensión de certificados

FIRMASEGURA S.A.S revocará o suspenderá un certificado cuando se cumplan con las circunstancias y condiciones establecidas en el acápite 4.7.1 de la D.P.C.

Operación de la infraestructura de clave pública

FIRMASEGURA SAS garantizará el correcto funcionamiento de su infraestructura de clave pública, lo que incluye la administración de los certificados, claves y otros elementos relacionados con la seguridad de la información. Asimismo, se encargará de garantizar la confidencialidad e integridad de la información que circule a través de su infraestructura, de acuerdo con los procedimientos definidos en la presente DPC.

Verificación de los certificados

FIRMASEGURA SAS verificará la autenticidad y validez de los certificados emitidos, mediante el uso de herramientas y métodos apropiados. Se garantizará que los certificados emitidos cumplen con las políticas y normas establecidas en la presente DPC, y se mantendrá un registro de las actividades de verificación

realizadas.

La empresa implementa sistemas de resguardo y protección contra siniestros para los documentos y equipos involucrados en los procesos de certificación, tales como sistemas de alimentación ininterrumpida (UPS) y sistemas de respaldo de información en línea y fuera de línea.

Se implementan controles de acceso físico y lógico para proteger los sistemas y la información contra posibles ataques, intrusiones o amenazas.

Además, se establecen procedimientos para la verificación y autenticidad de los certificados, de manera que se evita la falsificación o manipulación de la información.

8.5.3 Políticas de auditoría y monitoreo

FIRMASEGURA S.A.S. cuenta con las siguientes políticas y procedimientos establecidos para realizar auditorías y monitoreo constante de su infraestructura y servicios de certificación. Se realizan auditorías anuales internas y externas para validar la seguridad y confiabilidad de los sistemas, se monitorean constantemente los servidores y sistemas de backup para detectar cualquier tipo de vulnerabilidad y se establecen medidas de respuesta y recuperación en caso de incidentes de seguridad.

A continuación se detallan nuestras Políticas y Procedimientos de Auditoría y Monitoreo

Auditoría de Seguridad:

a. Planificación de Auditoría Anual:

El equipo de auditoría de seguridad definirá un plan anual que incluirá las áreas de enfoque, los sistemas y servicios a auditar, y los recursos necesarios.

b. Auditoría Física y Lógica:

Los auditores realizarán auditorías anuales tanto físicas como lógicas de la infraestructura, incluyendo la revisión de políticas, procedimientos y configuraciones de seguridad.

c. Pruebas de Penetración:

Se llevarán a cabo pruebas de penetración anualmente para identificar vulnerabilidades y evaluar la resistencia de los sistemas a posibles ataques por parte de personal especializado en esta actividad.

d. Revisión de Registros de Actividad:

Los registros de actividad serán revisados mensualmente en busca de actividades inusuales o sospechosas.

e. Informe de Auditoría:

Se generará un informe de auditoría que incluirá hallazgos, recomendaciones y acciones correctivas. El informe se compartirá con la alta dirección y se mantendrá como registro.

Monitoreo Continuo:

a. Configuración de Herramientas de Monitoreo:

Se configurarán herramientas de monitoreo para supervisar registros de actividad, alertas de seguridad, rendimiento del sistema y disponibilidad.

b. Revisión de Registros de Actividad:

Los administradores de seguridad revisarán periódicamente de manera quincenal los registros de actividad y responderán a eventos o alertas inusuales.

c. Respuesta a Incidentes:

El personal de respuesta a incidentes estará disponible para coordinar respuestas a eventos de seguridad.

Registro de Actividad y Eventos:

a. Generación de Registros:

Se generarán registros detallados de todas las operaciones y eventos relevantes, incluyendo el acceso a sistemas críticos, la emisión de certificados y cambios en la configuración.

b. Almacenamiento Seguro:

Los registros se almacenarán de forma segura y se protegerán contra modificaciones no autorizadas.

c. Acceso Restringido:

Solo el personal autorizado tendrá acceso a los registros de actividad y eventos.

Respuesta a Incidentes:

a. Detección de Incidentes:

Se implementarán herramientas para detectar incidentes de seguridad, incluyendo intrusiones o actividad anómala.

b. Notificación de Incidentes:

Se notificará a las partes pertinentes sobre los incidentes de seguridad tan pronto como sean detectados.

c. Evaluación y Mitigación:

Se llevará a cabo una evaluación de cada incidente y se implementarán medidas de mitigación según sea necesario.

Auditorías Internas y Externas:

a. Planificación de Auditorías Internas:

Se planifican auditorías internas anuales para evaluar el cumplimiento de políticas y procedimientos de seguridad.

b. Auditorías Externas:

Se permitirán auditorías externas realizadas por empresas auditoras debidamente calificadas con una periodicidad anual, con el fin de evaluar la seguridad y el cumplimiento.

Evaluación de Cumplimiento:

a. Revisión de Cumplimiento:

Se llevarán a cabo evaluaciones regulares para asegurarse de que la CA cumple con los requisitos legales y normativos aplicables.

b. Acciones Correctivas:

Si se identifican incumplimientos, se implementarán acciones correctivas según los procedimientos establecidos.

Retención de Registros:

a. Periodo de Retención:

Los registros de auditoría y monitoreo se retendrán por un período de cinco años, y se almacenarán de forma segura.

Capacitación y Concientización:

a. Programa de Capacitación:

Se implementará un programa de capacitación semestral para el personal involucrado en operaciones de la CA en materia de seguridad y auditoría.

Revisión y Actualización:

a. Revisión Anual:

La política se revisará y actualizará anualmente, o cuando ocurran cambios significativos en la infraestructura o en las operaciones de la CA.

8.5.4 Políticas de control de cambios

FIRMASEGURA S.A.S. cuenta con políticas y procedimientos establecidos para la gestión de cambios en su infraestructura y servicios de certificación. Se establecen controles de cambios que incluyen la evaluación de impacto de los mismos, la autorización previa de cambios críticos y la documentación de todos los cambios realizados.

Nuestra Política y Procedimientos de Gestión de Cambios se detalla a continuación:

Identificación y Registro de Cambios:

a. Se establece un registro de cambios para documentar todas las propuestas de cambios en la infraestructura y servicios.

b. Cualquier miembro del personal que identifique la necesidad de un cambio debe registrar la solicitud en el registro de cambios.

Evaluación de Impacto:

a. Cada solicitud de cambio será evaluada para determinar su impacto en la infraestructura y servicios de la CA, incluyendo consideraciones de seguridad y disponibilidad.

b. Los cambios se clasifican en tres categorías según su impacto potencial:

- Cambios Menores: Cambios con impacto mínimo.
- Cambios Significativos: Cambios con impacto moderado.
- Cambios Críticos: Cambios con impacto sustancial o potencialmente crítico.

Autorización Previa de Cambios Críticos:

a. Los cambios críticos requerirán autorización previa antes de ser implementados.

b. Un comité de autorización de cambios, que incluirá a representantes de seguridad, operaciones y gestión, revisará y aprobará o rechazará los cambios críticos.

c. Los cambios aprobados se registrarán en el registro de cambios.

Planificación de Cambios:

Se elaborará un plan detallado para cada cambio propuesto, incluyendo la descripción del cambio, los pasos a seguir, los recursos necesarios y un cronograma.

Implementación de Cambios:

a. Los cambios se implementarán siguiendo el plan previamente establecido.

b. Los cambios críticos se implementarán bajo la supervisión de un equipo de implementación que incluirá expertos en seguridad y otros expertos pertinentes.

Documentación de Cambios Realizados:

a. Se mantendrá una documentación detallada de todos los cambios realizados, incluyendo la descripción del cambio, fecha y hora de implementación, los resultados de las pruebas de validación y cualquier incidencia o problema detectado durante la implementación.

Pruebas y Validación:

Antes de implementar cambios, se realizarán pruebas de validación para asegurarse de que los cambios no afecten negativamente la operación de la CA.

Auditoría de Cambios:

Los cambios realizados serán objeto de auditoría y revisión para garantizar que se han implementado según lo planificado y que no han tenido impacto negativo en la infraestructura y servicios.

Comunicación de Cambios:

Se notificará a todas las partes interesadas sobre los cambios realizados, especialmente en el caso de cambios críticos que podrían afectar a usuarios o clientes.

Retiro de Cambios No Autorizados:

Si se detecta un cambio no autorizado, se revertirá y se tomarán medidas correctivas.

Revisión de Cambios Realizados:

Se realizará una revisión post-implementación de todos los cambios para evaluar su éxito y garantizar que los objetivos se hayan cumplido.

Retención de Documentación:

La documentación de todos los cambios realizados se retendrá por un período de 5 años.

Evaluación y Mejora Continua:

Se llevará a cabo una revisión periódica de los procedimientos de gestión de cambios para mejorar el proceso y adaptarlo a las necesidades cambiantes de la CA.

8.5.5 Políticas de cumplimiento y mejora continua

FIRMASEGURA S.A.S. tiene un compromiso con el cumplimiento normativo y la mejora continua de sus procesos y servicios. Para ello, cuenta con una serie de políticas y procedimientos internos que aseguran la conformidad con los estándares y regulaciones aplicables, y establecen mecanismos para la mejora continua.

Nuestras políticas de Cumplimiento y Mejora Continua se detallan a continuación:

Política de Cumplimiento:

La CA se compromete a cumplir con todas las leyes, regulaciones y estándares aplicables relacionados con la emisión y gestión de certificados de firma electrónica. Se buscará la máxima conformidad con las normativas de seguridad y confiabilidad de la industria para lo cual se seguirá el siguiente procedimiento:

a. Evaluación de Cumplimiento: La CA realizará evaluaciones anuales para garantizar el cumplimiento de todas las leyes, regulaciones y estándares relevantes. Esto incluye la identificación de requisitos legales y regulatorios aplicables.

b. Actualización de Políticas y Procedimientos: Cualquier cambio en las leyes, regulaciones o estándares aplicables se reflejará en las políticas y procedimientos de la CA. Se asignará la responsabilidad de mantenerse actualizado con los cambios normativos.

c. Auditorías de Cumplimiento: Se llevarán a cabo auditorías internas y externas anuales para evaluar el cumplimiento con los requisitos legales y regulatorios. Los resultados de las auditorías se utilizarán para implementar acciones correctivas y mejorar las prácticas.

d. Gestión de Riesgos de Cumplimiento: Se implementa el siguiente programa de gestión de riesgos de cumplimiento para identificar y mitigar los riesgos asociados con el incumplimiento de las normativas:

1. Identificación de Riesgos:

a. Se llevará a cabo una revisión exhaustiva de las normativas, leyes y regulaciones aplicables a la emisión de certificados de firma electrónica al menos una vez al año.

b. Se identificarán los riesgos potenciales de incumplimiento asociados con cada requisito normativo producto de la revisión.

2. Evaluación de Riesgos:

a. Se calificarán los riesgos identificados según su probabilidad de ocurrencia y su impacto potencial.

b. Los riesgos se categorizarán en función de su gravedad, prioridad y alcance.

3. Mitigación de Riesgos:

a. Se desarrollarán planes de mitigación para abordar los riesgos identificados.

b. Los planes de mitigación incluirán acciones específicas, responsables, plazos y recursos necesarios.

4. Implementación de Planes de Mitigación:

a. Los planes de mitigación se implementarán siguiendo un proceso estructurado.

b. Se realizará un seguimiento del progreso y se verificará la efectividad de las medidas tomadas.

5. Auditoría de Cumplimiento:

a. Se llevarán a cabo auditorías periódicas de cumplimiento para evaluar la efectividad de las medidas de mitigación y el cumplimiento general, con una periodicidad anual.

b. Los resultados de las auditorías se utilizarán para realizar ajustes y mejoras en el programa de gestión de riesgos.

6. Comunicación y Concientización:

a. Se fomentará la comunicación y la concienciación sobre riesgos de cumplimiento en toda la organización.

b. El personal será informado sobre los riesgos identificados y las medidas de mitigación correspondientes.

7. Registro y Documentación:

Se mantendrá un registro detallado de todos los riesgos identificados, evaluaciones de riesgos, planes de mitigación y acciones tomadas.

8. Revisión y Evaluación Continua:

El programa de gestión de riesgos se revisará y evaluará de manera continua, al menos una vez al año, para asegurarse de que esté actualizado y efectivo.

9. Cumplimiento Legal y Regulatorio:

Se garantizará el cumplimiento de los requisitos legales y regulatorios relacionados con la gestión de riesgos de cumplimiento.

Política de Mejora Continua:

La CA se compromete a mejorar continuamente sus operaciones y procesos con el fin de mantener y aumentar la calidad, eficiencia y seguridad en la emisión de certificados de firma electrónica basada en el siguiente procedimiento:

a. Identificación de Oportunidades de Mejora: Se establece el siguiente proceso para la identificación de oportunidades de mejora en todos los aspectos de las operaciones de la CA, incluyendo procesos, procedimientos y tecnologías.

1. Evaluación de Procesos y Procedimientos:

a. Se realizará una revisión exhaustiva de todos los procesos y procedimientos relacionados con la emisión de certificados de firma electrónica de manera anual.

b. Se identificarán áreas donde los procesos pueden ser más eficientes, seguros o rentables.

2. Análisis de la Tecnología Utilizada:

a. Se llevará a cabo un análisis de la infraestructura tecnológica utilizada en la CA, incluyendo AWS Private CA y otros sistemas, una vez al año.

b. Se evaluará la eficiencia y la capacidad de la tecnología para satisfacer las necesidades actuales y futuras de la CA.

3. Recopilación de Comentarios y Retroalimentación:

a. Se recopilarán comentarios y retroalimentación del personal involucrado en las operaciones de la CA, así como de los titulares de certificados y otras partes interesadas una vez al año.

b. Se alentará la comunicación abierta y la presentación de sugerencias de mejora.

4. Comparación con Mejores Prácticas del Sector:

a. Se compararán las operaciones de la CA con las mejores prácticas del sector de seguridad y certificación de firma electrónica una vez al año.

b. Se identificarán áreas donde la CA puede adaptar sus operaciones para estar alineada con las mejores prácticas.

b. Establecimiento de Objetivos de Mejora: La CA definirá anualmente objetivos medibles de mejora que aborden áreas específicas identificadas como oportunidades para un mejor desempeño.

c. Implementación de Mejoras: Las mejoras se implementarán siguiendo un proceso estructurado. Esto incluirá la asignación de responsabilidades, cronogramas y recursos necesarios.

d. Seguimiento y Medición: Se realizará un seguimiento y medición de los resultados de las mejoras implementadas para evaluar su impacto y efectividad.

e. Revisión y Evaluación: Se llevarán a cabo revisiones trimestrales de las mejoras implementadas para determinar su éxito y ajustar los enfoques según sea necesario.

f. Participación del Personal: Se fomentará la participación del personal en la identificación de oportunidades de mejora y se promoverá una cultura de mejora continua en toda la organización.

g. Comunicación de Mejoras: Se informará a las partes interesadas sobre las mejoras implementadas y sus beneficios.

h. Evaluación de la Efectividad: La CA evaluará continuamente la efectividad de las mejoras implementadas y buscará formas de optimizar aún más las operaciones.

8.5.6 Política de Protección de Datos Personales

FIRMASEGURA S.A.S. posee la siguiente política de Protección de Datos Personales:

Introducción

En FIRMASEGURA S.A.S., nos comprometemos a proteger la privacidad y los datos personales de nuestros usuarios. Esta política establece las directrices y los procedimientos para el manejo de datos personales, de acuerdo con la Ley Orgánica de Protección de Datos del Ecuador y otras regulaciones aplicables.

Definiciones

Datos personales: Cualquier información que identifique o haga identificable a una persona natural.

Titular de los datos: Persona natural o jurídica a quien corresponden los datos personales, corresponde a nuestro Emisor o suscriptor del servicio.

Tratamiento de datos: Cualquier operación o conjunto de operaciones realizadas sobre datos personales.

Principios de protección de datos personales

En el manejo de datos personales, nos regimos por los siguientes principios:

Licitud y consentimiento: Obtenemos el consentimiento del titular de los datos antes de recopilar, almacenar o utilizar sus datos personales. Este consentimiento debe ser libre, informado, expreso y específico para

cada finalidad. El texto del consentimiento se detalla a continuación:

FIRMASEGURA S.A.S. en cumplimiento con la ley Orgánica de Protección de Datos Personales, tiene como objetivo el precautelar el derecho que tienen sus clientes y usuarios, así como la ciudadanía en general, a la privacidad y protección de sus datos personales, que incluye el acceso y decisión sobre la información y datos de este carácter, así como su correspondiente protección. En este sentido, como titular de datos personales, el cliente o usuario debe consentir a FIRMASEGURA S.A.S. para tratar sus datos personales, con la finalidad de que dicha entidad le brinde un servicio con calidad y calidez, garantizando el cumplimiento de las normas vigentes y la protección de sus datos personales.

Por lo expuesto, como titular de datos personales, autorizo a FIRMASEGURA S.A.S., de forma expresa, de manera libre y voluntaria, específica e inequívoca, conforme al marco jurídico vigente, para que mis datos personales que hayan sido proporcionados de manera directa, indirecta, o que consten en bases de datos se traten de la siguiente forma:

1.-Para que puedan ser agrupados, segmentados, organizados, recopilados en una base de datos, y en general a darle el uso a su información personal, de conformidad a lo previsto en las normas vigentes, especialmente en todo lo previsto en la Ley Orgánica de Protección de Datos Personales.

2.-Para que puedan compartirse o comunicarse a terceros permitidos por la Ley, sean personas naturales, jurídicas o públicas, para los fines específicamente requeridos en la calidad de cliente o usuario del servicio de FIRMASEGURA S.A.S., las autoridades competentes a las cuales se les podrá suministrar datos son principalmente, pero no limitadas a: Agencia de Regulación y Control de las Telecomunicaciones, Fiscalía General del Estado, Autoridad de Protección de Datos Personales, y Ministerio de Telecomunicaciones y Sociedad de la Información como son integraciones para validar la identidad, integraciones con el Registro Civil para validación de cédulas de identidad, integraciones para prueba de vida, inteligencia artificial para funcionalidades específicas, o en general a los productos o servicios que FIRMASEGURA S.A.S. ofrezca; para optimizar sus funcionalidades, análisis, generación de modelos de información y/o perfiles de comportamiento actual y predictivo, procesos de debida diligencia, o en general cualquier otra revisión que se requiera para dichos fines.

3.-Para que puedan compartirse o comunicarse en aquellos procesos en que FIRMASEGURA S.A.S. deba atender para cumplir con la regulación ecuatoriana, sea de Arcotel, tributaria, societaria o financiera pertinente, o sus propias políticas internas; de igual manera los que realice con compañías de servicios auxiliares, para el cumplimiento de fines directamente relacionados con sus funciones o facultades y del destinatario, o de forma general los que cumpla de forma directa o a través de un tercero proveedor, tales como: servicios de pagos y cobros, servicios de mensajería SMS o correo electrónico u otros, informes de mejoras del sistema, actualizaciones, para el desarrollo de funcionalidades o de servicios en beneficio del cliente y usuario.

4.-Declaro que la información sobre mis datos personales que suministro y registro en FIRMASEGURA S.A.S. es exacta, cierta y verdadera.

5.-En caso de desear revocar esta autorización, de manera completa o parcial, entiendo y acepto que deberé comunicarlo a FIRMASEGURA S.A.S. La revocatoria no comprenderá en ningún caso los datos anónimos segregados o consolidados, ni podrá revocarse la autorización respecto a la información necesaria para el correcto funcionamiento del servicio que siga manteniendo con

FIRMASEGURA S.A.S. o información que fue tratada anteriormente en base a esta autorización, o la información que la empresa deba mantener de conformidad con la Ley.

Limitación de la finalidad: Los datos personales serán recopilados y utilizados solo para los fines específicos para los cuales se ha obtenido el consentimiento del titular y que son necesarios para ofrecer el servicio que minegocio.com.ec ofrece, mejorar la calidad, satisfacción y que ayuden a cumplir el propósito del servicio, a menos que la ley disponga lo contrario.

Calidad de los datos: Mantendremos los datos personales precisos, actualizados y completos, y tomaremos las medidas razonables para corregir o suprimir aquellos que sean inexactos o estén desactualizados. Para lo cual de manera periódica se solicitará a los emisores o suscriptores actualizar sus datos.

Seguridad: Mantenemos medidas técnicas, organizativas y legales adecuadas para proteger los datos personales contra pérdida, robo, acceso no autorizado, divulgación, alteración o destrucción. Estas medidas se detallan a continuación:

Medidas técnicas de Acceso y autenticación seguros: Tenemos sistemas de autenticación, validación y revocación sólidos para garantizar la integridad y confidencialidad de los datos.

Encriptación de datos: Poseemos técnicas de encriptación para proteger los datos personales tanto en tránsito como en reposo. Esto incluye el uso de protocolos seguros (como HTTPS) para la transmisión de datos y el almacenamiento encriptado de datos personales críticos.

Monitoreo y detección de intrusiones: Hemos implementado herramientas y técnicas de monitoreo y detección de intrusiones para identificar y responder rápidamente a posibles intentos de acceso no autorizado o actividades sospechosas en nuestros sistemas.

Respaldo y recuperación de datos: Poseemos procedimientos de respaldo de los datos, así como réplicas en tiempo real de nuestras bases de datos, para asegurar la disponibilidad y la integridad de los datos en caso de eventos adversos, conforme se puede observar en el acápite 8.9.1

Medidas organizativas:

Capacitación y concientización: Realizaremos programas de capacitación y concientización periódicos para todo el personal y para nuestros suscriptores enfocados en las mejores prácticas de protección de datos, la importancia de la privacidad y la seguridad de la información.

Políticas internas claras: Poseemos procedimientos internos para el manejo de datos personales, incluyendo aspectos como el acceso autorizado, el uso adecuado de los sistemas, la gestión de contraseñas y la clasificación de información.

Evaluaciones periódicas de riesgos: Realizamos evaluaciones de riesgos de seguridad de la información para identificar vulnerabilidades y tomar medidas correctivas o preventivas según corresponda.

Control de proveedores: Implementamos medidas de estricto control y supervisión de nuestros proveedores de servicios, asegurándonos de que cumplan con estándares adecuados de seguridad y privacidad.

Medidas legales:

Política de términos, condiciones y privacidad: Poseemos una política de condiciones y privacidad clara y accesible que explique cómo se recopilan, utilizan, almacenan y protegen los datos personales de los usuarios y que es aceptada por nuestros clientes.

Acuerdos de confidencialidad: Poseemos acuerdos de confidencialidad con nuestros empleados y colaboradores que involucren el acceso a datos personales, asegurando que se mantenga la confidencialidad de la información.

Cumplimiento normativo: Mantenemos actualizada nuestra política de protección de datos personales para cumplir con la Ley Orgánica de Protección de Datos del Ecuador y otras regulaciones aplicables.

Transparencia y acceso: Informamos a los titulares de los datos sobre el tratamiento de sus datos personales, incluyendo los fines, plazos de retención y derechos que les asisten. Asimismo, facilitamos el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición.

Responsabilidades y Obligaciones

Responsable de Protección de Datos: El Gerente General de FIRMASEGURA S.A.S. es el Responsable de Protección de Datos (RPD) encargado de supervisar y garantizar el cumplimiento de esta política y la normativa aplicable.

Capacitación y Concientización: Capacitamos y sensibilizamos constantemente a nuestro personal sobre la importancia de la protección de datos personales, así como sobre las responsabilidades y obligaciones que les competen.

Evaluación de Riesgos: Realizamos evaluaciones periódicas de los riesgos relacionados con el tratamiento de datos personales y adoptamos las medidas necesarias para mitigarlos.

Notificación de Violaciones de Datos: En caso de una violación de datos personales, notificaremos a la autoridad competente y al titular de los datos afectados, de acuerdo con los plazos y procedimientos establecidos por la ley. Tomaremos las medidas necesarias para mitigar los efectos de la violación y prevenir futuros incidentes.

Contratos de Confidencialidad: Poseemos acuerdos de confidencialidad con nuestros empleados que involucren el acceso o tratamiento de datos personales, asegurando que cumplan con las obligaciones de confidencialidad y seguridad establecidas por la ley.

Retención de Datos: Mantendremos los datos personales únicamente durante el tiempo necesario para cumplir con los fines para los cuales fueron recopilados, a menos que exista una obligación legal o requerimiento distinto.

Derechos del Titular de los Datos

Reconocemos los derechos del titular de los datos personales y nos comprometemos a garantizar su ejercicio. Estos derechos incluyen el acceso, rectificación, cancelación, oposición, limitación del tratamiento y portabilidad de los datos. Facilitaremos los medios para que los titulares de los datos puedan ejercer sus derechos de manera efectiva y sin obstáculos injustificados.

Responsabilidad del Uso de Datos por parte de los Suscriptores

FIRMASEGURA S.A.S. se compromete a garantizar la protección y confidencialidad de los datos personales recopilados para prestar sus servicios.

Actualización de la Política

Esta política será revisada periódicamente y actualizada según sea necesario, para garantizar su adecuación a los cambios en la legislación o en nuestras prácticas de tratamiento de datos personales.

Contacto

Preguntas, inquietudes o solicitudes relacionadas con la protección de datos personales, puede comunicarse con nuestro Responsable de Protección de Datos a través del correo electrónico datos@firmaseguraec.com

8.6 Componentes de seguridad perimetral

8.6.1 Sistema de prevención de intrusos

El Sistema de Prevención de Intrusos (IPS) desempeña un papel fundamental en la seguridad de la infraestructura alojada en GCP al monitorear y proteger la red contra intrusiones y actividades maliciosas. A continuación, se detallan las características específicas del servicio de IPS de GCP, junto con su funcionamiento en este entorno:

Implementación en GCP:

El servicio de IPS de GCP se implementa directamente en la infraestructura de Google Cloud. Esto permite una supervisión en tiempo real del tráfico de red que llega.

Detección de Amenazas en Tiempo Real:

El IPS en GCP utiliza una combinación de firmas, patrones y análisis de comportamiento para detectar amenazas en tiempo real. Esta capacidad de detección incluye la identificación de ataques basados en firmas conocidas y comportamientos inusuales.

Reglas Personalizadas:

Se pueden establecer reglas de política personalizadas para el IPS en GCP. Esto permite adaptar la seguridad a las necesidades específicas de la CA y definir acciones a tomar cuando se detectan amenazas.

Integración con Servicios de Seguridad de GCP:

El IPS se integra con otros servicios de seguridad de GCP, como el Firewall de Aplicaciones Web (WAF) y las Herramientas de Identidad y Seguridad de Google, para proporcionar una protección integral contra amenazas en la nube.

Escalabilidad Automatizada:

El servicio de IPS de GCP puede escalar automáticamente según las necesidades de tráfico, lo que garantiza un rendimiento óptimo en todo momento.

Registro y Auditoría Integrados:

El IPS registra todas las actividades y alertas, lo que facilita la revisión y el cumplimiento de los requisitos de auditoría. Estos registros son fundamentales para el análisis posterior y la identificación de tendencias de amenazas.

Gestión Centralizada:

A través del panel de control de GCP, se puede administrar de manera centralizada la configuración y las políticas del IPS en toda la infraestructura de la CA.

Actualizaciones Continuas:

Las bases de datos de firmas y patrones se actualizan automáticamente, lo que garantiza que el IPS esté al día con las amenazas emergentes.

Alertas y Respuesta a Incidentes:

El IPS puede generar alertas en tiempo real cuando se detectan amenazas y, según la configuración, tomar medidas automáticas para mitigar los riesgos. Esto puede incluir la interrupción del tráfico malicioso.

Evaluación de Riesgos y Mejora Continua:

Se realizan evaluaciones periódicas de riesgos y se implementan mejoras basadas en la retroalimentación y las tendencias de amenazas. Esto garantiza que el IPS siga siendo efectivo con el tiempo.

8.6.2 Firewall

El Firewall desempeña un papel esencial en la seguridad de la infraestructura alojada en GCP al controlar y filtrar el tráfico de red entrante y saliente. A continuación, se detallan las características específicas del servicio de Firewall de GCP, junto con su funcionamiento en este entorno:

Implementación en GCP:

El Firewall de GCP se implementa directamente en la infraestructura de Google Cloud. Esto permite la gestión centralizada y el control del tráfico de toda la red.

Reglas Personalizadas:

Se pueden definir reglas de Firewall personalizadas para adaptar la seguridad a las necesidades específicas de la CA. Esto incluye la configuración de reglas de filtrado basadas en dirección IP, puertos y protocolos.

Control de Acceso Basado en Etiquetas:

El Firewall de GCP permite el control de acceso basado en etiquetas de recursos. Puedes asignar etiquetas a tus recursos de GCP y aplicar reglas de Firewall específicas a esos recursos.

Reglas de Acceso en la Nube:

El Firewall de GCP también admite reglas de acceso en la nube que permiten restringir el tráfico sólo a ciertas direcciones IP o rangos de direcciones.

Vigilancia en Tiempo Real:

El Firewall de GCP proporciona una vista en tiempo real de las conexiones de red entrantes y salientes. Puedes usar esto para monitorear y analizar el tráfico en busca de actividad inusual o amenazas.

Escalabilidad y Alta Disponibilidad:

El Firewall de GCP es escalable y se adapta automáticamente a las demandas de tráfico. Además, está diseñado para ser altamente disponible y resistente a fallos.

Integración con Herramientas de Seguridad de GCP:

El Firewall se integra con otras herramientas de seguridad de GCP, como Cloud Security Command Center y la Herramienta de Identidad y Seguridad de Google.

Registro y Auditoría Integrados:

Todas las actividades del Firewall se registran y pueden ser revisadas posteriormente para cumplir con los requisitos de auditoría. Los registros son fundamentales para la detección de amenazas y el análisis posterior.

Políticas de Seguridad Basadas en Identidad:

Se pueden establecer políticas de seguridad basadas en identidad utilizando la autenticación y la autorización de GCP para reforzar el control de acceso.

Actualizaciones Continuas:

Google Cloud actualiza regularmente las reglas y definiciones del Firewall para mantenerse al día con las amenazas emergentes y las mejores prácticas de seguridad.

Respuesta a Incidentes Automatizada:

Se puede configurar el Firewall para tomar medidas automáticas en respuesta a eventos de seguridad, como bloquear tráfico malicioso o generar alertas.

8.6.3 Balanceadores

Los Balanceadores de Carga son componentes críticos para la seguridad y el rendimiento de la CA alojada en GCP. A continuación, se detallan las características específicas del servicio de Balanceador de Carga de GCP y cómo funcionan en este entorno:

Implementación en GCP:

El servicio de Balanceador de Carga de GCP se implementa en la infraestructura de Google Cloud para distribuir el tráfico de red de manera equitativa y asegurar la alta disponibilidad de tus aplicaciones y servicios de CA.

Equilibrio de Carga por Zonas:

El Balanceador de Carga de GCP admite el equilibrio de carga por zonas, lo que garantiza que el tráfico se dirija a las instancias de tu CA distribuidas geográficamente.

Equilibrio de Carga Global:

Puedes configurar un Balanceador de Carga Global que distribuye el tráfico a nivel mundial entre múltiples regiones, lo que mejora el rendimiento y la resistencia a fallos.

Redireccionamiento de Tráfico:

El Balanceador de Carga de GCP puede redirigir tráfico a instancias de backend específicas, lo que permite una gestión más efectiva de las solicitudes.

Balanceo de Carga Basado en Reglas:

Se definen reglas personalizadas para el Balanceador de Carga que direccionan el tráfico en función de criterios específicos, como rutas URL o cabeceras HTTP.

Monitoreo y Salud de Instancias:

El Balanceador de Carga verifica constantemente la salud de las instancias de backend y dirige el tráfico solo a las instancias en buen estado.

Escalabilidad Automatizada:

El Balanceador de Carga de GCP se escala automáticamente según las demandas de tráfico, lo que asegura un rendimiento óptimo en todo momento.

Integración con SSL:

El Balanceador de Carga de GCP admite la terminación SSL/HTTPS, lo que permite la encriptación de extremo a extremo para la seguridad de las comunicaciones.

Registros y Auditoría:

Se registran todas las actividades del Balanceador de Carga y se pueden revisar para el análisis posterior y el cumplimiento de los requisitos de auditoría.

Actualizaciones Continuas:

Google Cloud actualiza regularmente el servicio de Balanceador de Carga para mantenerse al día con las mejores prácticas de seguridad y las necesidades de rendimiento.

Integración con Herramientas de Seguridad de GCP:

El Balanceador de Carga se integra con otras herramientas de seguridad de GCP, lo que permite una protección integral de tu infraestructura de CA.

Respuesta a Incidentes Automatizada:

Se configura el Balanceador de Carga para redireccionar automáticamente el tráfico lejos de instancias no saludables en respuesta a eventos de seguridad.

8.7 Esquema de seguridad perimetral

Ver la sección: 6.1.2 Dispositivos de seguridad de borde

8.8 Esquema de seguridad de la infraestructura de clave pública

La infraestructura de PKI se encuentra desplegada bajo los servicios de Google Cloud Platform, por lo tanto sus servicios cumplen con diferentes lineamientos de seguridad que se detallan en los siguientes enlaces:

General: https://cloud.google.com/docs/security/overview/whitepaper?hl=es-419

Infraestructura: https://cloud.google.com/docs/security/infrastructure/design?hl=es-419

8.9 Plan de contingencia

8.9.1 Plan de Contingencia para Casos de Emergencia y Desastres (DCP):

El objetivo principal del Plan de Contingencia es garantizar una respuesta rápida y efectiva en situaciones de emergencia o desastres que puedan interrumpir las operaciones normales de la entidad de certificación (CA). A continuación, se describen los procedimientos detallados para el DCP:

8.9.1.1 Evaluación de Riesgos y Amenazas:

Identificación de riesgos y amenazas específicas que podrían afectar a la CA, incluyendo ciberataques, desastres naturales, fallos de hardware, etc.

8.9.1.2 Equipos de Respuesta a Emergencias:

Designación de un Equipo de Respuesta a Emergencias (ERT) con roles y responsabilidades claramente definidos.

Establecimiento de un líder del ERT y un sistema de comunicación de emergencia.

8.9.1.3 Procedimientos de Respuesta:

8.9.1.3.1 Emergencia por Ataque Cibernético:

Detección y notificación inmediata de un ataque cibernético.

Aislamiento y contención del ataque.

Análisis forense para determinar la causa y el alcance del ataque.

Implementación de medidas correctivas y restauración de servicios.

8.9.1.3.2 Emergencia por Desastre Natural:

Evaluación de la situación y seguridad del personal.

Activación de sistemas de respaldo y migración a un sitio seguro.

Restauración de servicios en el sitio de respaldo cuando sea seguro hacerlo.

8.9.1.4 Respaldo y Recuperación de Datos:

Realización de copias de seguridad de claves privadas y datos críticos.

Almacenamiento seguro de copias de seguridad en ubicaciones fuera del sitio principal.

Procedimientos detallados de restauración de datos y validación.

Los procedimientos de Respaldos y Recuperación se los detalla en el acápite 8.16.

8.9.1.5 Protección de Claves Privadas:

Utilización de Hardware de Seguridad (HSM) para el almacenamiento seguro de claves privadas.

Implementación de protocolos de seguridad para el acceso a claves sensibles.

Los procedimientos de Respaldos y Recuperación se los detalla en el acápite 8.16.1 y 8.16.2.

8.9.1.6 Comunicación y Notificación:

Establecimiento de un sistema de notificación interno y externo en caso de emergencia.

Definición de la cadena de mando para la toma de decisiones durante una crisis.

8.9.1.7 Capacitación y Simulacros:

Entrenamiento del ERT en los procedimientos de respuesta.

Realización de simulacros para evaluar la efectividad del DCP.

8.9.1.8 Evaluación y Actualización Continua:

Revisión y actualización periódica del DCP en función de cambios en riesgos y lecciones aprendidas de eventos pasados.

8.9.1.9 Detección y Notificación:

Se implementará un sistema de monitoreo constante para detectar cualquier fallo de conexión con GCP. Si se detecta un fallo, se notificará de inmediato al equipo de operaciones de la CA.

8.9.1.10 Investigación y Diagnóstico:

Se llevará a cabo una investigación exhaustiva para determinar la causa del fallo de conexión. Esto puede incluir la revisión de registros y la colaboración con el equipo de soporte de GCP.

8.9.2 Plan de Contingencia GCP:

FIRMASEGURA trabaja con una plataforma en la nube que brinda herramientas para una recuperación rápida ante desastres. Los servicios operan bajo recursos de alta disponibilidad que ante un error de hardware se podrá seguir con disponibilidad del negocio.

En caso de presentarse una contingencia se consideran los siguientes puntos:

- Asignación de nuevas IPS públicas con rápida propagación mediante cloudflare en caso de problemas de conectividad con la región del balanceador de carga.
- En caso de falla en la región de los servicios de Google Cloud Platform se podrán mover los servicios a regiones cercanas mediante configuraciones de base de datos y GKE.
- A nivel de servicios externos (Registro civil, IA) si no se encuentran disponibles se crearán procesos de cola para operaciones de validaciones manuales.

8.9.2.1 Comunicación con Usuarios:

En caso de una interrupción prolongada de los servicios de la CA, se notificará a los usuarios afectados y se proporcionarán instrucciones sobre cómo proceder, incluyendo la posible reubicación de servicios a un entorno de respaldo.

8.9.2.2 Restablecimiento y Recuperación:

Una vez que se haya restablecido la conexión con GCP, se llevarán a cabo pruebas de verificación para asegurarse de que todos los sistemas y servicios estén funcionando correctamente. Se restaurarán los servicios en línea tan pronto como sea posible.

8.10 Plan de Continuidad del Negocio (BCP)

El objetivo del Plan de Continuidad del Negocio es garantizar la continuidad de las operaciones de la CA en situaciones de interrupción, independientemente de la causa, manteniendo la disponibilidad de los servicios críticos y protegiendo la integridad de los certificados electrónicos. A continuación, se describen los planes detallados para el BCP:

8.10.1 Identificación de Procesos Críticos:

Identificación y priorización de los procesos y servicios críticos relacionados con la generación y gestión de certificados de firmas electrónicas.

8.10.2 Prevención:

Implementación de medidas preventivas para reducir el riesgo de interrupciones, como seguridad cibernética sólida, mantenimiento preventivo de equipos, etc.

8.10.3 Resiliencia de TI:

Diseño de una infraestructura de TI con redundancia y alta disponibilidad.

Planificación de la migración de sistemas críticos a ubicaciones de respaldo.

8.10.4 Gestión de la Cadena de Suministro:

Identificación de proveedores críticos y establecimiento de acuerdos de continuidad con ellos.

Mantenimiento de inventarios de hardware y software críticos.

8.10.5 Comunicación y Notificación:

Establecimiento de un sistema de comunicación interno y externo para notificar a las partes interesadas en caso de interrupción.

8.10.6 Capacitación y Simulacros:

Realización de capacitaciones y simulacros para mantener al personal preparado para actuar en situaciones de interrupción.

8.10.7 Evaluación y Actualización Continua:

Revisión y actualización periódica del BCP para mantenerlo alineado con los cambios en la organización y los riesgos.

8.11 Procedimientos para la Recuperación ante Desastres (DRP - Disaster Recovery Procedures):

Evaluación Inicial:

Evaluación inicial de la situación para determinar si se deben activar los procedimientos de recuperación ante desastres.

Activación de la Recuperación:

Activación de los sistemas y equipos de recuperación, siguiendo los planes establecidos en el BCP.

Recuperación de Sistemas y Datos:

Procedimientos detallados para restaurar sistemas y datos críticos según los RTO y RPO definidos en el BCP.

Verificación de la Integridad de los Datos:

Verificación de la integridad de los datos recuperados y revisión exhaustiva para identificar cualquier posible pérdida o daño.

Reanudación de las Operaciones:

Procedimientos para reanudar las operaciones esenciales de acuerdo con el plan de prioridades establecido en el BCP.

Monitoreo y Evaluación Post Recuperación:

Monitoreo continuo de los sistemas y operaciones para garantizar que todo funcione correctamente después de la recuperación.

Documentación y Lecciones Aprendidas:

Documentación de los procedimientos específicos seguidos durante la recuperación y registro de lecciones aprendidas para futuras mejoras.

8.12 Procedimiento para Realizar Pruebas de Contingencia: Planificación de las Pruebas de Contingencia:

Se definen los objetivos específicos de las pruebas de contingencia, incluyendo los escenarios de interrupción que se simularán (pérdida de datos, ciberataques, etc.).

Se identifican los sistemas y servicios críticos de FIRMASEGURA S.A.S. que se someterán a pruebas.

Se designa un equipo de pruebas que incluya personal técnico, de seguridad y gestión.

Se establece un calendario de pruebas que minimice el impacto en las operaciones normales de FIRMASEGURA S.A.S.

Preparación:

Se documenta el plan de pruebas de contingencia detallado que incluye escenarios de prueba específicos, roles y responsabilidades, y los criterios de éxito para cada prueba.

Se notifica a todo el personal de FIRMASEGURA S.A.S acerca de las próximas pruebas de contingencia y se proporciona información sobre su propósito y alcance.

Simulación de Escenarios:

Se simulan los escenarios de interrupción de acuerdo con el plan de pruebas.

Se observa y registra el comportamiento de la plataforma en respuesta a cada escenario de prueba. Esto puede incluir la pérdida de acceso a datos críticos, la caída de sistemas, etc.

Activación del Plan de Contingencia:

Cuando se identifica un escenario de interrupción, se activará el plan de contingencia de FIRMASEGURA S.A.S. de acuerdo con el procedimiento establecido.

Se seguirá los pasos detallados en el plan de contingencia para garantizar la continuidad de las operaciones relacionadas por FIRMASEGURA S.A.S.

Evaluación y Análisis:

Se evalúa la efectividad del plan de contingencia en cada escenario de prueba. Se registra cualquier dificultad o desafío que surja durante la activación del plan.

Se identifican áreas de mejora en los procedimientos, sistemas o políticas en base a las lecciones aprendidas durante las pruebas.

Recuperación y Restauración:

Después de completar cada prueba de contingencia, se restaurarán los sistemas y servicios afectados a su estado normal.

Se verificará que los datos y las configuraciones no se hayan dañado durante las pruebas.

Documentación y Reporte:

Se debe documentar los resultados de las pruebas, incluyendo cualquier problema identificado, acciones tomadas y lecciones aprendidas.

Se preparará un informe de pruebas de contingencia que resuma los hallazgos y las recomendaciones para

mejorar el plan de contingencia y las operaciones de FIRMASEGURA S.A.S.

Revisión y Actualización del Plan de Contingencia:

Basándose en los resultados de las pruebas, se revisará y actualizará el plan de contingencia de FIRMASEGURA S.A.S. según sea necesario.

Asegurarse de que todas las recomendaciones de mejora se incorporen en el plan.

Capacitación y Concientización:

Se proporcionará capacitación continua al personal de FIRMASEGURA S.A.S. sobre los procedimientos de contingencia y los cambios realizados en el plan.

Se fomentará la conciencia sobre la importancia de la preparación para contingencias.

Programación de Pruebas Regulares:

Se programará pruebas de contingencia de forma regular, al menos anualmente, para mantener la preparación y la eficacia del plan de contingencia.

8.13 Sistema de control de acceso al centro de cómputo

Acceso Físico:

Medidas de Seguridad Física: Los centros de datos de GCP cuentan con medidas de seguridad física robustas que incluyen sistemas de autenticación y autorización para garantizar que solo el personal autorizado pueda ingresar a las instalaciones.

Identificación y Autenticación: El personal que necesita acceder a las áreas críticas del centro de cómputo debe someterse a un proceso de identificación y autenticación riguroso, que puede incluir tarjetas de acceso, verificación biométrica y autenticación multifactorial.

Control de Acceso Lógico:

Políticas de Seguridad y Roles: GCP establece políticas de seguridad sólidas y utiliza modelos de seguridad basados en roles (RBAC) para definir quién puede acceder a qué recursos y realizar qué acciones. Estas políticas son altamente personalizables y se aplican de manera granular.

Auditoría y Registros: GCP mantiene registros detallados de todas las actividades de acceso y acciones realizadas en la infraestructura. Los registros son esenciales para la monitorización continua y las auditorías de seguridad.

Autenticación Multifactorial (MFA): GCP fomenta el uso de la autenticación multifactorial (MFA) para reforzar la seguridad de la autenticación, especialmente en cuentas de alto privilegio.

GCP mantiene un alto nivel de seguridad en sus centros de datos y utiliza una combinación de medidas de control de acceso físico y lógico, auditorías y capacitación del personal para garantizar la seguridad de su infraestructura y los activos críticos. La seguridad es una parte fundamental de sus operaciones.

8.14 Registro ingreso centro de cómputo

Registro de Acceso: En los centros de datos de GCP, se mantiene un registro completo de todos los ingresos. Cada vez que alguien accede a las instalaciones, se registra su entrada, lo que incluye su identificación, fecha y hora de ingreso, así como otros detalles relacionados con la visita.

Sistema de Registro: Google Cloud utiliza sistemas de registro electrónicos avanzados para garantizar la precisión y disponibilidad de la información de acceso. Estos registros son cruciales para la seguridad y la capacidad de respuesta a incidentes.

8.15 Dispositivos utilizados para el acceso al centro de cómputo

Tarjetas de Acceso Electrónico: El acceso al centro de cómputo de GCP se controla mediante el uso de tarjetas electrónicas de acceso. Estas tarjetas son emitidas a personal autorizado y se utilizan para desbloquear puertas y acceder a áreas específicas.

Verificación Biométrica: En áreas críticas, es común que GCP implemente sistemas de verificación biométrica, como escaneo de huellas dactilares o reconocimiento facial, para garantizar la autenticación adicional de los empleados y visitantes.

Autenticación Multifactorial (MFA): En algunos casos, se pueden utilizar dispositivos MFA, como llaveros o aplicaciones móviles, para verificar la identidad del personal autorizado.

Cámaras de Vigilancia: GCP emplea sistemas de cámaras de vigilancia para monitorear y registrar visualmente todas las actividades de acceso en sus instalaciones. Estas cámaras se utilizan tanto para la seguridad como para auditorías posteriores.

8.16 Respaldo de información

8.16.1 Respaldos de Claves Privadas:

Al utilizar HSM administrado por AWS private CA se opera bajo el procedimiento establecido por AWS.

8.16.2 Respaldos de Claves Públicas:

Las claves públicas de los certificados se respaldarán de forma diaria. Para ello, se seguirán los siguientes procedimientos:

a. El personal autorizado generará copias de seguridad diarias de las claves públicas.

b. Las claves privadas se almacenarán y se gestionarán en el HSM administrado por AWS.

c. Antes de almacenar las copias de seguridad, se cifrarán utilizando algoritmos de cifrado fuertes y se protegerán las claves de cifrado.

d. Se mantendrán registros precisos de todos los respaldos de certificados, incluyendo detalles como el número de serie del certificado y la fecha de respaldo.

8.16.3 Evaluación y Mantenimiento:

La efectividad de los procedimientos de respaldo y recuperación será evaluada anualmente.

Pruebas de recuperación se llevarán a cabo semestralmente para garantizar que los respaldos sean funcionales.

8.16.4 Cumplimiento y Auditoría:

Se mantendrá un registro completo de todas las operaciones de respaldo y recuperación, que estará disponible para fines de auditoría.

Se llevarán a cabo auditorías anuales para asegurarse de que la política se cumpla de manera adecuada.

8.16.5 Formación y Concientización:

Se proporcionará formación regular al personal involucrado en las operaciones de respaldo y recuperación.

Se promoverá la conciencia de seguridad en torno a la importancia de esta política.

8.16.6 Acceso

Solo personal autorizado y debidamente autenticado tendrá acceso conforme se detalla a continuación:

8.16.6.1Roles de Personas Autorizadas:

Administradores de Seguridad de la CA: Estos son responsables de la gestión de la infraestructura de seguridad de la CA, incluyendo el control de acceso a los respaldos. Sus roles y responsabilidades incluyen:

Aprobar solicitudes de acceso a respaldos de claves privadas y certificados.

Realizar auditorías y supervisar el cumplimiento de la política.

Supervisar las operaciones de respaldo y recuperación.

Mantener registros de acceso y auditoría.

Operadores de Respaldos: Este personal es responsable de la realización de las operaciones de respaldo programadas y de garantizar la seguridad de las copias de seguridad. Sus roles y responsabilidades incluyen:

Generar copias de seguridad de claves privadas y certificados siguiendo la programación establecida.

Cifrar y almacenar de forma segura las copias de seguridad.

Mantener registros detallados de los respaldos realizados.

Personal de Recuperación: Este personal es responsable de autorizar y llevar a cabo las operaciones de recuperación de claves y certificados en caso de necesidad. Sus roles y responsabilidades incluyen:

Evaluar y aprobar las solicitudes de recuperación, asegurando que el solicitante proporcione información de autenticación válida.

Llevar a cabo procesos de recuperación utilizando claves de recuperación seguras y procesos de autenticación sólidos.

8.16.6.2Motivos para Acceso Autorizado:

Las personas autorizadas pueden acceder a los respaldos en los siguientes casos:

Respaldo Programado: Los operadores de respaldos tienen acceso autorizado para llevar a cabo respaldos de claves privadas y certificados de acuerdo con la programación establecida.

Recuperación de Claves o Certificados: El personal de recuperación puede acceder a los respaldos en caso de que se requiera la recuperación de datos.

Auditoría y Supervisión: Los administradores de seguridad de la CA pueden acceder a los registros y a los respaldos con fines de auditoría y supervisión para garantizar el cumplimiento de la política.

8.16.6.3Procedimiento para Control de Acceso Autorizado:

Solicitud de Acceso: Cualquier solicitud de acceso a respaldos debe ser presentada por el personal autorizado a los administradores de seguridad de la CA. La solicitud debe incluir una justificación válida y

detalles sobre el motivo del acceso.

Evaluación y Aprobación: El personal de seguridad de la CA evaluará y aprobará la solicitud de acceso. Esto incluirá verificar que la solicitud esté respaldada por motivos legítimos y que el solicitante esté debidamente autenticado.

Realización de la Operación: Una vez aprobada, la operación de acceso autorizado se llevará a cabo de acuerdo con los procedimientos establecidos. Se mantendrán registros detallados de la operación.

Auditoría y Registro: Cada acceso autorizado se registrará y se mantendrá un registro detallado, incluyendo la fecha, la hora, el motivo y el personal involucrado en la operación.

8.16.7 Protección

Los certificados emitidos se protegerán mediante la firma electrónica de la CA utilizando sus claves privadas.

Los certificados emitidos se protegerán contra la alteración no autorizada.

8.16.8 Revocación

En caso de que se sospeche que una clave privada se ha comprometido o perdido, se procederá a revocar el certificado correspondiente de inmediato.

Se seguirán los procedimientos de revocación de certificados de acuerdo con las políticas de la CA.

8.17 Manejo y resolución de solicitudes y problemas

Se dispone de un sistema de seguimiento y gestión de solicitudes y problemas relacionados con los certificados.

Se establecen procedimientos para la resolución de solicitudes y problemas. Se mantendrá a los solicitantes informados sobre el estado de sus solicitudes y problemas.

Recepción y Registro de Problemas:

a. Los problemas relacionados con los certificados pueden ser reportados por los titulares de certificados, terceros de confianza o detectados internamente.

b. Los problemas se registrarán de manera detallada, incluyendo la fecha, hora, el nombre del reportante y la descripción del problema.

Evaluación Inicial del Problema:

a. Un equipo de soporte de certificados realizará una evaluación inicial del problema para determinar su naturaleza y gravedad.

b. Se clasificarán los problemas en categorías, como problemas de seguridad, problemas de validez del certificado, entre otros.

Asignación de Recursos:

a. El equipo de soporte asignará recursos para abordar y resolver el problema de acuerdo a su categoría y gravedad.

b. Se designará un responsable para liderar el proceso de resolución del problema.

Investigación y Análisis:

a. Se llevará a cabo una investigación detallada para analizar la causa del problema.

b. Se verificarán los registros y la documentación relevante, y se recopilará la información necesaria.

Resolución del Problema:

a. Con base en los resultados de la investigación, se tomarán medidas para resolver el problema de manera eficiente y efectiva.

b. Si es necesario, se aplicarán medidas correctivas para abordar la causa raíz del problema.

Comunicación con los Titulares de Certificados:

a. En caso de problemas que afecten a los titulares de certificados, se proporcionará una comunicación clara y oportuna sobre el estado de resolución del problema y las acciones necesarias.

Registros y Documentación:

Se mantendrán registros detallados de todos los problemas reportados y las acciones tomadas para resolverlos.

Seguimiento y Revisión:

a. Se realizará un seguimiento de los problemas resueltos para garantizar que no vuelvan a ocurrir.

b. Se llevará a cabo una revisión de los procedimientos de manejo y resolución de problemas para identificar oportunidades de mejora una vez al año.

Capacitación y Concientización:

El personal involucrado en el manejo y resolución de problemas recibirá capacitación en mejores prácticas y procedimientos de seguridad.

Cumplimiento Legal y Regulatorio:

Se garantizará el cumplimiento de los requisitos legales y regulatorios relacionados con el manejo de problemas de certificados.

9 Contacto

Gerente General: SCBC CORP S.A.S.

Teléfono: 032466888

Dirección: Ambato, Calabazas e Higos, 3er Piso.

Sitio Web: www.firmaseguraec.com