FIRMASEGURA S.A.S

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

VERSIÓN 1.0

PSI FIRMASEGURA S.A.S.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

CONTROL DE VERSIONES:

FECHA	AUTOR	VERSIÓN	DESCRIPCIÓN
19/10/2023	PAÚL ILLINGWORTH	1.0	VERSIÓN APROBADA

Contenido

1. Introducción

Esta Política de Seguridad de la Información (PSI) tiene como objetivo establecer los lineamientos y procedimientos necesarios para garantizar la protección y seguridad de la información en posesión de FIRMASEGURA S.A.S, entidad Certificadora (CA) ecuatoriana, que opera bajo la normativa de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL).

1.1. Objetivo de la PSI

El objetivo principal de la PSI es establecer los requisitos y medidas de seguridad necesarias para proteger la información relacionada con la emisión, gestión y revocación de certificados de firma electrónica, garantizando la confidencialidad, integridad y disponibilidad de los mismos, y asegurando la identificación y autenticación de los usuarios y dispositivos que interactúan con los sistemas y servicios de la CA.

1.2. Alcance de la PSI

Esta PSI es aplicable a todos los procesos, sistemas, aplicaciones y personas que intervienen en la emisión, gestión y revocación de certificados de firma electrónica, así como a la protección de la información en posesión de

FIRMASEGURA S.A.S, incluyendo los sistemas, redes, servidores, bases de datos, instalaciones físicas, y todo otro recurso tecnológico o humano involucrado en estos procesos.

1.3. Definiciones y Acrónimos

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

Algunos de las definiciones comunes en la terminología son:

Política de Seguridad de la Información (PSI): Conjunto de requisitos y medidas de seguridad que establecen las políticas, procedimientos, normas y controles necesarios para proteger la información en una organización.

Autoridad certificadora (CA): Una entidad confiable que emite certificados de firma electrónica 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 de firma electrónica.

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 digital que contiene la clave pública del titular del certificado de firma electrónica.

Certificado de revocación (CRL): Un certificado digital 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 RAIZ: Una Autoridad Certificadora Raíz es una entidad que emite certificados de firma electrónica 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 de firma electrónica 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

GCP: Google Cloud Platform

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

EJBCA: Enterprise JavaBeans Certificate Authority

PGP: Pretty Good Privacy

GPG: GNU Privacy Guard

PKCS: Public Key Cryptography Standards

EKU: Extended Key Usage

OID: Object Identifier

DSA: Digital Signature Algorithm

RSA: Rivest–Shamir–Adleman encryption algorithm

ECC: Elliptic Curve Cryptography

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

1.4. Descripción del servicio de firma electrónica

1.4.1. Descripción general del servicio de firma electrónica

El servicio de firma electrónica que ofrecerá FIRMASEGURA S.A.S será un servicio de Certificación de Autoridad (CA) que emitirá certificados de firma electrónica para personas naturales y jurídicas en Ecuador. Los certificados se emitirán de acuerdo con los estándares y regulaciones establecidos por la legislación ecuatoriana.

El servicio de firma electrónica que ofrecerá FIRMASEGURA S.A.S. permitirá a los usuarios firmar documentos electrónicos con validez jurídica. Los certificados serán emitidos utilizando la tecnología de Infraestructura de Clave Pública (PKI) y se gestionarán mediante la plataforma de EJBCA alojada 100% en Google Cloud Platform (GCP).

1.5. Tipos de certificados que se emitirán

FIRMASEGURA S.A.S emitirá dos tipos de certificados de firma electrónica:

- Certificado para persona natural en archivo .P12
- Certificado para representante legal de persona jurídica en archivo .P12

1.6. Descripción de los certificados que se emitirán

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.

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.

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.

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

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

1.7. Procedimiento de solicitud, emisión, renovación y revocación de certificados

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.

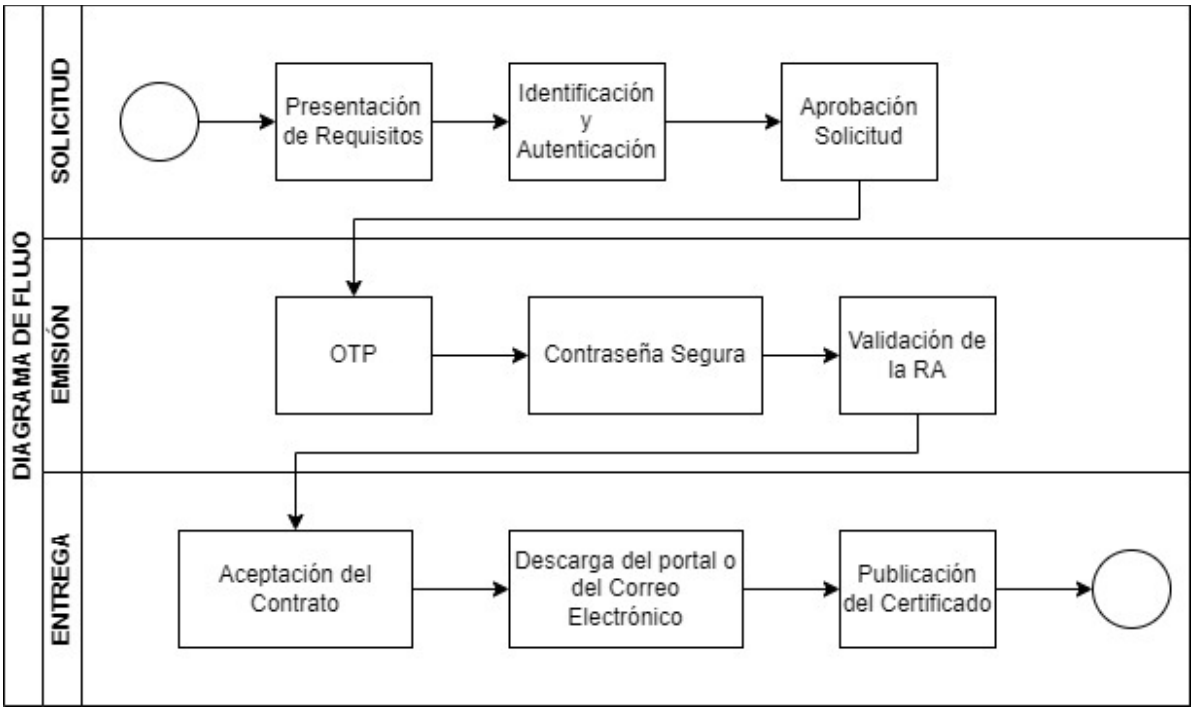
Emisión: Una vez validada la identidad del solicitante, se genera un link de descarga para el certificado de firma electrónica en formato .p12 el cual podrá descargarlo desde la plataforma, previa validación por OTP y una vez que asigne una contraseña segura, además es enviado al correo electrónico proporcionado por el solicitante. Este proceso se detalla en el acápite 1.9. del presente documento.

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 del mismo.

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



A continuación, se detalla cada uno de los procesos:

1.8. Solicitud de certificados

1.8.1. 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.

1.8.2. 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.

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 Políticas de Certificación y las Condiciones Generales de Contratación.

1.8.3. 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 electrónicos o 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 2.3 del presente documento.

1.8.4. 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 a lo que se especificará en la Política de Certificación correspondiente a cada tipo de certificado.

1.8.5. 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 4.8 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.

1.9. Emisión de certificados

1.9.1. 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 la clave pública en formato PKCS #10 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.

1.9.2. 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.

1.10. Aceptación del certificado

1.10.1. 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 firmado y el certificado haya sido entregado al Suscriptor, ya sea personal o telemáticamente.

Como evidencia de la aceptación, deberá quedar constancia física o digital de la aceptación del Suscriptor. El certificado se considerará válido a partir de la fecha en que se dio la aceptación.

1.11. 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.

1.12. Uso de las claves y el certificado

1.12.1. Uso de la clave privada y del certificado por el Suscriptor

Los certificados podrán ser utilizados según lo estipulado 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.

1.12.2. 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 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.

1.13. 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.

1.14. 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.

1.15. 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 la

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.

1.16. Notificación de la emisión del certificado renovado

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

1.17. Forma de aceptación del certificado renovado

El certificado se aceptará al firmar electrónicamente la renovación.

1.18. 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.

1.19. 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.

1.20. 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.

1.20.1. 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 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 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 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 DPC o en la PC

correspondiente.

1.20.2. 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.

1.20.3. 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.

1.20.4. 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, un formulario web desde el que podrá realizar y tramitar la solicitud de revocación de su certificado.

Este mecanismo de solicitud de revocación se convierte en el principal para todos los certificados emitidos, de tal forma que se garantiza que cualquier certificado puede ser revocado en menos de 24 horas.

El proceso de revocatoria por parte del propio suscriptor es online:

- El Suscriptor deberá ingresar en la plataforma de la CA con los datos con los que se registró para emitir su certificado de firma electrónica.

- Deberá escoger la opción revocatoria de certificado del menú de opciones y registrará la solicitud de revocatoria.

- Personal de soporte a usuarios recibirá la solicitud y validará su identidad, para esta validación de identidad se realizará una video llamada en la cuál se confirmará que se trata de quien dice ser.

- Se procederá de forma inmediata a revocar el certificado del Suscriptor.

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 recibirá una comunicación del sistema informando que se ha producido la revocación del certificado.

1.20.5. Procedimientos internos

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.

1.20.6. 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.

1.20.7. 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.

1.20.8. Frecuencia de emisión de las CRL

La CRL de los certificados de entidad final se emite cada 24 horas. La CA Raíz emitirá también una CRL cada 2 horas.

1.20.9. 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.

1.20.10. 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.

1.20.11. 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 CA 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.

1.21. Requisitos técnicos de los certificados

Los certificados emitidos por FIRMASEGURA S.A.S cumplirán con los siguientes requisitos técnicos:

- El certificado será generado utilizando el estándar X.509 v3.
- El certificado tendrá una longitud de clave mínima de 2048 bits.
- El algoritmo de firma utilizado será SHA-256 o superior.

- El certificado incluirá el nombre y la información de contacto de FIRMASEGURA S.A.S. como entidad emisora.
- El certificado incluirá la información del titular del certificado, incluyendo su nombre, dirección y número de identificación.
- El certificado incluirá la clave pública del titular del certificado.
- El certificado incluirá una fecha de inicio y una fecha de vencimiento.
- El certificado incluirá un número de serie único.
- El certificado será emitido para un propósito específico, como la firma electrónica de documentos o la autenticación de usuarios en línea.
- El certificado será emitido en formato de archivo PKCS #12, token o en nube para su fácil instalación en los sistemas del titular del certificado.

2. Proceso de validación de identidad

Para la identificación de la persona natural se exigirá su validar que se trata de 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 o 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.

2.1.3.1. 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 CA verifica la autenticidad de estos documentos.

Entrevista en Persona: En algunos casos, especialmente para certificados que se utilizarán en aplicaciones de alto riesgo, la CA puede requerir 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.

De igual manera para validar información de personas naturales con RUC o

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.

3. Seguridad y protección de la información

3.1. Medidas de seguridad física y lógica para la protección de la información

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.

Se implementan controles de acceso y autenticación para la gestión y acceso a los datos personales.

Asimismo, 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.

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 periódicas de seguridad 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 con láser.

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.

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.

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 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.

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 terceros de confianza 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 mensual 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.

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:

a. 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:

a. 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:

a. 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:

a. 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:

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

Revisión de Cambios Realizados:

a. 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:

a. La documentación relacionada a todos los cambios realizados se retendrá por un período de cinco años.

Evaluación y Mejora Continua:

a. 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.

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 cuál 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:

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

8. Revisión y Evaluación Continua:

a. El programa de gestión de riesgos se revisará y evaluará de manera continua para asegurarse de que esté actualizado y efectivo.

9. Cumplimiento Legal y Regulatorio:

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

6. 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 EJBCA 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.

7. Procedimientos para el manejo y custodia de las claves privadas

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 y copias de seguridad.

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 13.

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 8.1.

b. Se establecerán procedimientos para controlar y auditar el acceso a las claves privadas.

Cumplimiento Legal y Regulatorio:

a. Se garantizará 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 mensualmente 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, al menos 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 1.20 del presente documento.

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 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 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. Política de gestión de claves

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 detalla a continuación:

8.1. Políticas de Acceso y Autenticación:

Se establece la política de acceso estricta para el HSM. Solo usuarios y sistemas autorizados deben tener acceso al HSM.

Utilizar autenticación multifactor (MFA) para garantizar que solo personal autorizado pueda acceder al HSM.

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.

Realizar operaciones de respaldo y recuperación de claves y certificados almacenados 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.

Coordinar y llevar a cabo la recuperación de claves y certificados en caso de un incidente.

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:

Implementar 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:

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

Actualizaciones y Parches:

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

9. Política de gestión de riesgos y contingencias

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:

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.

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.

9.1.3. Procedimientos de Respuesta:

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.

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.

9.1.3.3. 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 6.4.3.

9.1.3.4. 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 6.4.5.

9.1.4. 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.

9.1.5. Capacitación y Simulacros:

Entrenamiento en los procedimientos de respuesta.

Realización de simulacros para evaluar la efectividad del DCP.

9.1.6. Evaluación y Actualización Continua:

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

9.1.7. 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.

9.1.8. 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.

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 inmediata 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.

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.

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.

9.3. 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:

9.3.1. Identificación de Procesos Críticos:

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

9.3.2. Prevención:

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

9.3.3. 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.

9.3.4. 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.

9.3.5. Comunicación y Notificación:

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

9.3.6. Capacitación y Simulacros:

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

9.3.7. Evaluación y Actualización Continua:

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

9.4. 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.

9.5. 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 (fallos de hardware, 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.

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.

10. Procedimientos de Auditoría y Supervisión

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 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.

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 cómo se recopilará la evidencia durante las auditorías, qué registros se revisarán y cómo se documentarán los hallazgos.

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

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

11. Política de privacidad y protección de datos personales

11.1. Política de Protección de Datos Personales

FIRMASEGURA 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 e 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: 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 6.4.3.

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: Designamos al Ing. Paúl Illingworth CEO de la empresa como 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 paul.illingworth@firmaseguraec.com

12. Procedimiento para la gestión de reclamos y quejas

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:

a. 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.

Capacitación y Concientización:

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

Cumplimiento Legal y Regulatorio:

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

13. Respaldo de información

13.1. Respaldos de Claves Privadas:

Al utilizar HSM administrado por GCP se opera bajo el procedimiento establecido por Google Cloud Platform el cuál se detalla en su documentación del siguiente enlace:

https://cloud.google.com/docs/security/cloud-hsm-architecture?hl=es-419

13.2. 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 GCP.

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.

13.3. 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.

13.4. 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.

13.5. 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.

13.6. Acceso

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

13.7. Roles 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.

13.8. Motivos 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.

13.9. Procedimiento 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.

14. Procedimientos para la revisión y actualización de la PSI

14.1. Procedimientos para la revisión y actualización periódica de la PSI

FIRMASEGURA S.A.S establecerá un proceso de revisión y actualización periódica anual de la PSI para garantizar su adecuación y actualización con los requisitos normativos, tecnológicos y de seguridad vigentes.

La revisión y actualización periódica de la PSI será realizada por el equipo técnico y legal de FIRMASEGURA S.A.S, que deberá verificar la conformidad de la PSI con los cambios en las leyes y regulaciones aplicables, los avances tecnológicos y las buenas prácticas de seguridad y gestión de servicios de firma electrónica.

14.2. Procedimientos para la notificación de cambios a los usuarios del servicio

FIRMASEGURA S.A.S informará a los usuarios del servicio de firma electrónica sobre cualquier cambio que se realice en la PSI. La notificación se realizará por medio del sitio web de FIRMASEGURA S.A.S, donde se publicará la versión actualizada de la PSI.

Asimismo, los usuarios que hayan aceptado la PSI recibirán una notificación por correo electrónico en la dirección que hayan registrado, informándoles sobre la actualización de la PSI y los cambios que se hayan realizado. FIRMASEGURA S.A.S garantizará que los usuarios tengan acceso a la versión vigente de la PSI en todo momento, y mantendrá registros de las notificaciones realizadas a los usuarios.