FirmaSeguraEC

# DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN PARA CERTIFICADOS DE PERSONAS NATURALES

**VERSIÓN 1.0**

**DPC FIRMASEGURA S.A.S.**

# DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN PARA CERTIFICADOS DE PERSONAS NATURALES

**CONTROL DE VERSIONES:**

| FECHA | AUTOR | VERSIÓN | DESCRIPCIÓN |
|---|---|---|---|
| 20/10/2023 | PAÚL ILLINGWORTH | 1.0 | VERSIÓN APROBADA |

# 1 Objetivo

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

# 2 Introducción

FIRMASEGURA S.A.S es una entidad en proceso de solicitud para ser una Entidad Certificadora autorizada por el ARCOTEL que ofrece servicios de certificación de firmas electrónicas para personas naturales y representantes legales de empresas en Ecuador. La infraestructura de clave pública (PKI) utilizada por FIRMASEGURA S.A.S está basada en estándares internacionales y aplicando las mejores prácticas.

## 2.1 Alcance de la DPC

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

## 2.2 Terminología

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

Algunos de las definiciones comunes en la terminología son:

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

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

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

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

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

**Política de Certificación (PC):** Un documento que describe las prácticas y procedimientos

técnicos que la CA implementa para asegurar la integridad, confidencialidad, autenticidad y disponibilidad de la PKI.

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

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

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

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

Y los acrónimos más comunes son:

PKI: Public Key Infrastructure

CA: Certificate Authority

RA: Registration Authority

CRL: Certificate Revocation List

OCSP: Online Certificate Status Protocol

SCEP: Simple Certificate Enrollment Protocol

CMS: Cryptographic Message Syntax

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

SSL: Secure Sockets Layer

TLS: Transport Layer Security

S/MIME: Secure/Multipurpose Internet Mail Extensions

PGP: Pretty Good Privacy

GPG: GNU Privacy Guard

PKCS: Public Key Cryptography Standards

EKU: Extended Key Usage

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

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

# 3 Descripción de la infraestructura

### 3.1.1 Autoridades de Certificación (CA)

La CA raíz es la encargada de emitir certificados para las CA subordinadas y los certificados de usuarios y dispositivos.

### 3.1.2 Autoridad de Registro (AR o RA)

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

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

### 3.1.3 Autoridad de Validación (AV o VA)

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

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

### 3.1.4 Solicitante

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

### 3.1.5 Suscriptor

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

### 3.1.6 Custodio de claves

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

### 3.1.7 Tercero que confía en los certificados

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

## 3.2 Jerarquía entidad de certificación de información

La jerarquía de certificación de información tiene como objetivo controlar la seguridad adecuada para cada división de tareas de las CA que intervienen. Para la prestación de los servicios se establece una jerarquía de entidad de certificación de dos niveles que permite políticas de administración, control y seguridad.

### 3.2.1 FIRMASEGURA CA Raíz

Es la entidad de certificación raíz definida en la jerarquía que tiene como propósito emitir certificados a

otras entidades de certificación. Su certificado de llave pública es auto firmado.

### 3.2.2 FIRMASEGURA CA1 Subordinada

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

## 3.3 Administración de la autoridad de certificación

**Procedimientos de Emisión de Certificados:** La CA implementa procedimientos para la emisión de certificados de firma electrónica en formato .p12, que incluyen verificación de identidad, validación de solicitudes y generación segura de claves.

**Procedimientos de Revocación y Renovación:** Se establecen procedimientos claros para la revocación y renovación de certificados en caso de pérdida o vencimiento los cuales se detallan más adelante.

**Procedimientos de Auditoría de Seguridad:** Se realizan auditorías de seguridad regulares para evaluar el cumplimiento normativo y la integridad de la infraestructura los cuales se detallan más adelante.

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

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

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

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

### 3.3.2 Identificación y Autenticación para cada Usuario Autorizado

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

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

### 3.3.3 Roles que requieren Segregación de Funciones

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

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

### 3.3.4 Controles de Personal

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

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

confidencialidad.

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

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

### 3.4 Roles y responsabilidades para generación y migración de llaves privadas

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

#### 3.4.1 Rol Responsable de Generación de Claves Privadas:

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

**Responsabilidades:**

Generar claves privadas utilizando métodos criptográficos seguros y aleatorios.

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

**Requisitos de Autenticación:**

Debe autenticarse mediante credenciales seguras antes de generar claves privadas.

Se requiere autenticación de dos factores para tareas críticas.

#### 3.4.2 Rol Responsable de Migración de Llaves Privadas:

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

**Responsabilidades:**

Realizar la migración de llaves privadas siguiendo procedimientos seguros.

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

**Requisitos de Autenticación:**

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

### 3.5 Procesos de auditoría de seguridad

#### 3.5.1 Definición del Plan de Auditoría:

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

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

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

**Recursos Necesarios:**

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

### 3.5.2 Programa Definido:

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

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

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

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

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

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

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

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

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

### 4.1.1 Firma electrónica para personas naturales en archivo .p12:

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

Los tipos de certificado que FirmaSegura S.A.S. emite para personas naturales son los siguientes:

| Naturaleza de Persona | Tipo de Certificado | OID de Política |
|---|---|---|
| Personal Natural con o sin RUC | Certificado de Firma Electrónica | 1.3.6.1.4.1.61305.2.2.1 |

A continuación se muestra un listado de los elementos de un certificado de firma electrónica para Persona

Natural con o sin RUC.

| **Descripción** | **Elemento** | **Contenido** |
|---|---|---|
| Estructura Básica | | |
| 1.1 Versión | Version | 3 |
| 1.2 Número Serial | Serial Number | Valor generado automáticamente por la CA. |
| 1.3 Algoritmo de Firma | Signature Algoritm | SHA-256 with RSA |
| 1.4 Nombre Distintivo o DN del emisor | Issuer Distinguished Name | |
| 1.4.1 País | Country (C) | EC |
| 1.4.2 Organización | Organization (O) | FIRMASEGURA S.A.S. |
| 1.4.3 Unidad Organizacional | Organization Unit (OU) | ENTIDAD DE CERTIFICACIÓN DE INFORMACION |
| 1.4.4 Nombre del emisor | Common Name (CN) | AUTORIDAD DE CERTIFICACIÓN RAÍZ CA-1 FIRMASEGURA S.A.S. |
| 1.5 Validez | Validity | 20 años |
| 1.5.1 Desde | Not Before | Fecha de inicio de validez |
| 1.5.2 Hasta | Not After | Fecha de expiración |
| 1.6 Titular | Subject | |
| 1.6.1 País | Country (C) | País de residencia del titular |

| | | |
|---|---|---|
| 1.6.4 Nombre del titular | Common Name (CN) | Nombres completos del titular. |
| 1.6.5 Email | Email (E) | Email del titular. |
| 1.7 Serial Number | Serial Number (SN) | Número de serie generado en el proceso de validación de documentos. |
| 2. Extensiones | | |
| 2.1 Identificador de AC | Authority Key Identifier | |
| 2.1.1 Identificador | Key Identifier | Asignado por la CA |
| 2.2 Identificador de Titular | Subject Key Identifier | Asignado por la CA |
| 2.3 Usos permitidos | Key Usage | Digital Signature,<br>Non-Repudiation,<br>Key Encipherment |
| 2.4.2 Repositorio de Políticas | Policy Qualifier/ CPS Pointer | https://firmaseguraec.com/politicas_persona_natural |
| 2.5 Política de Certificado | | |
| 2.5.1 Identificador de Política | Policy Identifier | 1.3.6.1.4.1.61305.2.2.1 |
| 2.5.2 Repositorio de Políticas | Policy Qualifier/ CPS Pointer | https://firmaseguraec.com/politicas_persona_natural |
| 2.6 Restricciones Básicas | Basic Constraints | Subject is not a CA |
| 2.6.1 Autoridad Certificadora | CA | |
| 2.7 CRL | CRL Distribution Points | |
| 2.7.1 URL de distribución | Distribution Point | http://crl.firmaseguraec.com/crl/ |

| | | |
|---|---|---|
| | | ccce5a4f-6b68-46fc-a620-4abcc4c4a690.crl |
| 2.8 Acceso a información Authority Information Access | 2.9 Acceso a información Authority Information Access | |
| 2.8.1 Método de acceso Access Method | 2.9.1 Método de acceso Access Method | OID: 1.3.6.1.5.5.7.1.1 Online Certificate Status Protocol |
| 2.8.2 URL Alternative Name | Access Location | http://ocsp.firmaseguraec.com |
| 2.9 Otras extensiones | | |
| 2.9.1 Cédula de identidad | | 1.3.6.1.4.1.61305.3.1 |
| 2.9.2 Nombre(s) | | 1.3.6.1.4.1.61305.3.2 |
| 2.9.3 Primer Apellido | | 1.3.6.1.4.1.61305.3.3 |
| 2.9.4 Segundo Apellido | | 1.3.6.1.4.1.61305.3.4 |
| 2.9.5 Dirección | | 1.3.6.1.4.1.61305.3.7 |
| 2.9.6 Teléfono | | 1.3.6.1.4.1.61305.3.8 |
| 2.9.7 Ciudad | | 1.3.6.1.4.1.61305.3.9 |
| 2.9.8 País | | 1.3.6.1.4.1.61305.3.12 |
| 2.9.9 RUC | | 1.3.6.1.4.1.61305.3.11 |

### 4.1.2 Otros servicios relacionados

Además, se ofrecerán los siguientes servicios:

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

En un futuro se brindará el siguiente servicio:

- Plataforma para firmar electrónicamente documentos.

### 4.1.3 Periodos de validez de los certificados

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

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

### 4.1.4 Tarifas

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

## 4.2 Mecanismos de validación: CRL, OCSP, LDAP

### 4.2.1 Servicio de listas de certificados revocados (CRL)

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

### 4.2.2 Servicio consulta en línea de certificados electrónicos (OCSP)

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

La respuesta a una petición OCSP bajo el RFC mencionado provee la siguiente información acerca del estado de un certificado:

- Good: El certificado es válido.
- Revoked: El certificado está revocado.
- Unknown: El certificado no fue emitido por la CA de FIRMASEGURA.

### 4.2.3 Servicio repositorio de certificados electrónicos (LDAP)

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

## 4.3 Certificados de servidor seguro (SSL)

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

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

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

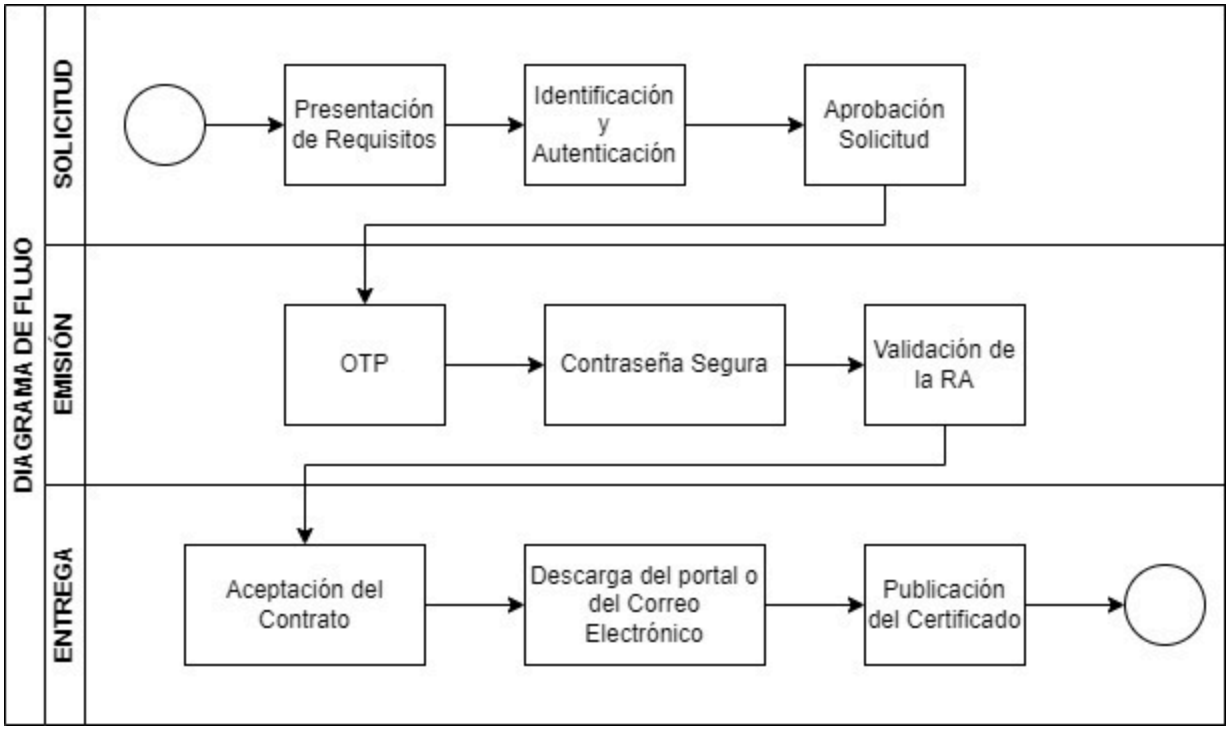
**Emisión:** Una vez validada la identidad del solicitante, se genera un link de descarga para el certificado de firma electrónica en formato .p12 el cual podrá descargarlo desde la plataforma, previa validación por OTP y una vez que asigne una contraseña segura, además es enviado al correo electrónico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

**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:




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

### 4.4.1 Solicitud de certificados

#### 4.4.1.1 Quién puede solicitar un certificado de Persona Natural

Podrán solicitarlo personas naturales y deberá llenar los siguientes requisitos:

- Tipo Documento
- Número de Identificación
- Primer y Segundo Nombre
- Apellido
- Apellido 2
- Código de huella dactilar de la cédula.
- Correo Electrónico
- Celular
- Fecha de nacimiento
- Sexo
- Dirección
- Datos de la Factura
- Foto de anverso de la cédula
- Foto del reverso de la cédula
- Selfie con cédula en mano
- Video otorgando autorización para emitir el certificado para mayores de 65 años.

#### 4.4.1.2 Proceso de solicitud de certificados

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

La CA proporcionará al Solicitante la siguiente información:

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

- Disponibilidad para realizar el proceso de registro.

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

- Acceder y aceptar las condiciones de contratación.

#### 4.4.1.3 Rango de validez del certificado de firma electrónica

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

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

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

#### 4.4.1.4 Identificación y Autenticación

Es responsabilidad de la CA realizar de forma fehaciente la identificación y autenticación del Suscriptor. Este proceso deberá ser realizado previamente a la emisión del certificado.

#### 4.4.1.5 Aprobación o denegación de las solicitudes de certificados

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

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

La validación de la identidad del solicitante será biométrica y documental, mediante el registro y procesamiento en la plataforma web de la CA.

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

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

Se procederá entonces a la emisión del certificado.

### 4.4.2 Emisión de certificados

#### 4.4.2.1 Acciones de la CA durante la emisión de los certificados

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

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

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

La RA enviará a la CA por un canal seguro la clave pública en formato PKCS #12 junto con el resto de los datos verificados que están contenidos en el certificado. Se procederá entonces a la generación del certificado en un procedimiento que utilizará protección contra falsificación y mantendrá la confidencialidad de los datos intercambiados.

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

#### 4.4.2.2 Notificación al Suscriptor de la emisión del certificado

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

### 4.4.3 Aceptación del certificado

#### 4.4.3.1 Forma en la que se acepta el certificado

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

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

#### 4.4.3.2 Publicación del certificado

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

### 4.4.4 Uso de las claves y el certificado

#### 4.4.4.1 Uso de la clave privada y del certificado por el Suscriptor

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

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

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

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

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

### 4.4.5 Renovación de certificados sin cambio de claves

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

### 4.4.6 Renovación con cambio de claves

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

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

### 4.4.7 Tramitación de las peticiones de renovación en línea

Se realizarán los siguientes pasos:

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

### 4.4.8 Notificación de la emisión del certificado renovado

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

### 4.4.9 Publicación del certificado renovado

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

## 4.5 Modificación de certificados

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

## 4.6 Revocación de certificados

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

### 4.6.1 Circunstancias para la revocación

Un certificado podrá ser revocado debido a las siguientes causas:

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

- Comprobación de que los datos contenidos en la solicitud del certificado son falsos o incorrectos.
- Modificación de cualquier dato contenido en el certificado.
- Extinción de la personalidad jurídica, o disolución de la entidad sin personalidad jurídica.

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

- Compromiso o sospecha de compromiso de la clave privada o de la infraestructura o sistemas de la CA, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
- Infracción por parte de la CA o de la RA de los requisitos previstos en los procedimientos de gestión de certificados establecidos en la DPC o en la PC correspondiente.
- Compromiso o sospecha de compromiso de la seguridad de la clave privada o del certificado.
- Acceso o utilización no autorizados por un tercero de la clave privada del certificado.
- El incumplimiento por parte del Suscriptor de las normas de uso del certificado expuestas en la presente DPC, en la PC correspondiente o en el instrumento jurídico vinculante entre la CA y el Suscriptor.
- En caso de que se advierta que los mecanismos criptográficos utilizados para la generación de la clave privada o el certificado no cumplen los estándares de seguridad mínimos necesarios para garantizar su seguridad.

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

- Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
- Pérdida o inutilización por daños del dispositivo criptográfico.
- Acceso no autorizado por un tercero a los datos de activación del dispositivo criptográfico.

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

d) Circunstancias que afectan al Suscriptor:

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

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

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

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

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

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

• El fallecimiento del Firmante.

• Solicitud escrita por Suscriptor.

e) Otras circunstancias:

• Resolución judicial o administrativa que lo ordene.

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

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

### 4.6.2 Quién puede solicitar la revocación

Pueden solicitar la revocación de un certificado:

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

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

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

Podrán tramitar la solicitud de revocación del certificado:

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

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

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

### 4.6.3 Procedimientos de solicitud de revocación

Existen distintas alternativas para solicitar la revocación de un certificado.

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

### 4.6.4 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 cual 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.

### 4.6.5 Procedimientos internos de revocación

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

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

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

### 4.6.6 Plazo en el que la CA debe procesar la solicitud de revocación

El tiempo máximo desde la recepción de la solicitud de revocación hasta su confirmación y tramitación

será de 24 horas. Si en ese tiempo no se puede confirmar la solicitud de revocación, ésta no será tramitada.

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

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

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

#### 4.6.8 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.

#### 4.6.9 Tiempo máximo entre la generación y la publicación de las CRL

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

#### 4.6.10 Disponibilidad de sistemas en línea de verificación del estado de los certificados

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

#### 4.6.11 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.

### 4.7 Servicios de información del estado de los certificados

#### 4.7.1 Características operativas

FIRMASEGURA S.A.S. ofrece un servicio gratuito de publicación en Web de Listas de Certificados Revocados (CRL), sin restricciones de acceso, así como en los certificados, en su extensión CRL Distribution Points.

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

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

### 4.7.2 Disponibilidad del servicio

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

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

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

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

### 4.7.3 Finalización de la suscripción

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

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

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

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

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

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

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

### 4.8.1 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 bajo su criterio que el solicitante se presente en persona para una entrevista de validación de identidad. Durante esta entrevista, se verifica la correspondencia de la persona con los documentos presentados y se toma una fotografía para comparación.

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

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

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

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

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

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

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

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

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

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

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

### 4.9 Políticas de retención de registros y de privacidad de la información del solicitante

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

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

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

### 4.10 Propósitos y usos de los certificados

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

### 4.11 Responsabilidades y obligaciones de los usuarios de certificados

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

• Utilizar el certificado únicamente para los fines previstos.

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

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

## 5 Autoridades de registro (AR)

### 5.1 Autoridad de registro o Registradoras (ARs o RAs)

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

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

Ofrecen y hacen uso de los servicios de la CA cumpliendo con las siguientes funciones:

- Verificar la identidad de un suscriptor, analizando la información proporcionada en la Solicitud de Certificado y comparando con fuentes adicionales de información.
- Validar documentos que sustentan la información
- Obtener información a partir de los servicios del Registro Civil del Ecuador o de otras Instituciones públicas.
- Aprobar o rechazar el registro de una solicitud.

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

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

### 5.1.1 Certificado de firma electrónica

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

**Autenticidad y Confianza:**

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

**Contenido del Certificado de firma electrónica:**

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

**Firma de la Entidad de Certificación (CA):**

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

### 5.1.2 Entidad de certificación

Es una plataforma que permite a las organizaciones establecer y gestionar su propia Autoridad de Certificación (CA) para emitir y gestionar certificados de firma electrónica.

**Autoridad de Certificación (CA):**

Aspectos clave de la entidad de certificación ofrecida:

**Emisión de Certificados de firma electrónica:**

Permite la emisión de una amplia gama de certificados de firma electrónica, incluidos firma electrónica, cifrado y autenticación.

**Cumplimiento de Normativas:**

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

**Escalabilidad:**

Es escalable y se adapta a las necesidades de diferentes organizaciones, desde pequeñas empresas

hasta grandes empresas y gobiernos.

**Interoperabilidad:**

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

**Administración de Ciclo de Vida de Certificados:**

Permite la gestión completa del ciclo de vida de los certificados, lo que incluye emisión, renovación, revocación y caducidad.

**Autenticación y Firma Electrónica:**

Admite la autenticación de usuarios y dispositivos mediante certificados de firma electrónica, lo que garantiza la seguridad en las comunicaciones y transacciones en línea.

**Seguridad de Claves:**

Proporciona una sólida seguridad para las claves privadas utilizadas en la emisión de certificados, lo que protege contra amenazas y ataques.

**Auditoría y Registro:**

Registra todas las operaciones críticas y permite la realización de auditorías para garantizar la conformidad y la seguridad.

**Soporte de Cifrado y Firmas Fuertes:**

Utiliza algoritmos de cifrado y firmas robustas para garantizar la seguridad de los certificados de firma electrónica emitidos.

**Flexibilidad y Personalización:**

Es altamente personalizable y se puede adaptar a las necesidades específicas de una organización, lo que permite la implementación de políticas y procedimientos a medida.

### 5.1.3 Algoritmos

**Algoritmo RSA:** Seguridad Asimétrica en la Comunicación

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

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

Este algoritmo es ampliamente utilizado en aplicaciones que requieren comunicaciones seguras, como

SSL/TLS para la protección de sitios web, correo electrónico seguro y firmas electrónicas. Para obtener más detalles técnicos sobre el algoritmo RSA, se puede consultar la página: https://datatracker.ietf.org/doc/html/rfc8017

**Algoritmo SHA:** Integridad y Verificación en la Criptografía

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

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

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

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

## 5.2 Contenedores criptográficos

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

**Almacén de Llaves (Keystore):**

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

**Formato PKCS#12 y Proceso de Certificación:**

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

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

### 5.3 Especificaciones técnicas de los contenedores

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

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

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

Normas y Estándares de Contenedores: Nuestros contenedores cumplen con las normas PKCS#12 y X.509, que establecen estándares ampliamente aceptados en la industria para la gestión de claves privadas y certificados digitales.

### 5.4 Estándares y normas internacionales

#### 5.4.1 Normas, estándares

##### 5.4.1.1 Leyes y regulaciones aplicables

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

##### 5.4.1.2 Políticas y estándares relacionados

FIRMASEGURA S.A.S seguirá las políticas y estándares relacionados con la seguridad de la información y la privacidad de los datos personales, incluyendo los estándares establecidos por la International Organization for Standardization (ISO) en las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013. Además, FIRMASEGURA S.A.S seguirá las políticas y estándares establecidos por el RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Campos Obligatorios en un Certificado de firma electrónica:**

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

**Datos del Certificado:**

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

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

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

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

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

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

Firma del Certificado:

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

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

Extensiones en un Certificado de firma electrónica:

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

**KeyUsage (Uso de Clave):**

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

AuthorityKeyIdentifier (Identificador de Clave de Autoridad):

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

**Certificate Policies (Políticas de Certificación):**

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

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

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

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

**Respuestas OCSP:**

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

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

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

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

**Datos de Solicitud OCSP (OCSP Request):**

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

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

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

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

**Extensiones Opcionales:** Pueden incluirse para requisitos o funciones específicas.

**Proceso de Respuesta OCSP:**

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

Verificación de la estructura de la solicitud.

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

Aseguramiento de que la solicitud contiene la información requerida.

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

**Componentes de una Respuesta OCSP:**

Una respuesta OCSP está compuesta por varios componentes esenciales:

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

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

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

**Extensiones Opcionales:** Se incluyen para funciones o requisitos específicos.

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

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

**Respuesta para Cada Certificado:**

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

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

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

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

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

#### 5.4.1.3 Contratos y acuerdos

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

#### 5.4.1.4 Requerimientos de privacidad y protección de datos personales

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

**Responsabilidad del Uso de Datos por parte de los Suscriptores**

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

**Actualización de la Política**

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

**Contacto**

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

## 6 Contacto

Gerente General: Paúl Illingworth

Correo electrónico: paul.illingworth@firmaseguraec.com

Teléfono: 032466888

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

Sitio Web: www.firmaseguraec.com