# POLITICA DE CERTIFICACION Y DECLARACIÓN DE PRÁCTICAS

**CONTENIDO**

# 1. INTRODUCCIÓN

SOFT & NET SOLUTIONS S.A.C., en adelante SoftNet, es una empresa peruana fundada en el 2007, dedicada a proveer soluciones integrales en alta tecnología con preponderancia en identidad digital, automatización de procesos, facturación electrónica y gestión de proyectos. Como parte de sus planes de expansión en la prestación de servicios, en el año 2020 se constituye como Entidad de Certificación, con lo cual es de las pocas empresas peruanas en brindar todas las variedades de productos y servicios que homologa INDECOPI a través de sus diversos procedimientos de acreditación dentro del marco de la Infraestructura Oficial de Firma Electrónica (IOFE)

## 1.1. OBJETIVO

Esta Política de Certificación y la Declaración de Prácticas de Certificación (PC y DPC) presentan los principios, procedimientos y prácticas empleados en la emisión y la gestión del ciclo de vida dentro de la Jerarquía de la EC de SoftNet. Esta PC y DPC y todas sus enmiendas se incorporan por referencia en los certificados emitidos bajo esta PC y DPC.

Esta PC y DPC es aplicable a todas las entidades relacionadas con la EC de SoftNet, incluidas las entidades de registro, los titulares, los suscriptores, y los terceros que confían. También se considera a otro tipo participante que pueda realizar algunas funciones relacionadas con la emisión y/o revocación de certificados, en nombre de los titulares. En tales casos, los principios, procedimientos y prácticas contenidos en este documento serán aplicables a dichos participantes, como si fueran suscriptores, en la medida de lo posible.

Esta PC y DPC especifica los principios, procedimientos y prácticas que la EC de SoftNet sigue, conforme a la CP y CPS de emSign y la Guía de Acreditación de Entidades de Certificación establecida por INDECOPI, para cumplir con las siguientes políticas, pautas y requisitos:

1. RFC 3647 del Internet Engineering Task Force (IETF) para la Política de Certificación y la Declaración de Práctica de Certificación.
2. Las últimas versiones (a fecha de este PC y DPC) de los requisitos de CA / Browser Forum (CABF) que incluyen: (Ref: https://cabforum.org)
3. Servicios de sellado de tiempo de acuerdo con RFC 3161 de IETF y otras normas aplicables.
4. Políticas de certificados de la lista de confianza aprobada de Adobe (AATL).
5. Programa de certificado raíz de Apple, requisitos de auditoría del programa de certificado raíz de confianza de Microsoft, política de tienda raíz de Mozilla, programa de certificado raíz de Java de Oracle y política de certificado raíz para los proyectos de Chromium.
6. Si existe alguna inconsistencia entre esta PC y DPC y los requisitos antes mencionados, entonces los requisitos mencionados tienen prioridad sobre esta CP y DPC.

## 1.2. NOMBRE DE DOCUMENTO E IDENTIFICACIÓN

El OID para emSign PKI es:
un iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) eMudhra Technologies Limited (50977) emSign PKI (1).

Los valores de identificador de objeto (OID) correspondientes al CP/CPS de emSign son los siguientes:

| Entidad / Política de Certificado | OID |
|---|---|
| Organization | 1.3.6.1.4.1.50977 |
| emSign PKI | 1.3.6.1.4.1.50977.1 |

| | |
|---|---|
| emSign CP/CPS Document | 1.3.6.1.4.1.50977.1.0.1 |

## 2. OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre la infraestructura y procesos de los servicios de certificación digital brindados por SoftNet a través de la infraestructura provista y administrada por el grupo eMudhra, la cual cuenta con certificación Webtrust for Certification Authorities emitida por AICPA/CICA.
SoftNet representa a eMudhra para todos los aspectos de mediación entre las personas naturales y jurídicas del Estado Peruano y la Entidad de Certificación emSign de eMudhra.

## 3. DEFINICIONES Y ABREVIACIONES

| | |
|---|---|
| Entidades de Certificación – EC | Persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. |
| Entidades de Registro o Verificación - ER | Persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, comprobación de éstos respecto a un solicitante de un mecanismo de firma electrónica o certificación digital, la aceptación y autorización de las solicitudes para la emisión de un mecanismo de firma electrónica o certificados digitales, así como de la aceptación y autorización de las solicitudes de cancelación de mecanismos de firma electrónica o certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente. |
| Política de Certificación (PC o CP) | Documento oficialmente presentado por una entidad de certificación a la Autoridad Administrativa Competente, mediante el cual establece, entre otras cosas, los tipos de certificados digitales que podrán ser emitidos, cómo se deben emitir y gestionar los certificados, y los respectivos derechos y responsabilidades de las Entidades de Certificación. Para el caso de una EC Raíz, la CP incluye las directrices para la gestión del Sistema de Certificación de las EC vinculadas. |
| Prácticas de Certificación | Prácticas utilizadas para aplicar las directrices de la política establecida en la CP respectiva. |
| Declaración de prácticas de certificación (DPC o CPS) | Documento oficialmente presentado por una entidad de certificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Certificación. |
| Acreditación | Acto a través del cual la Autoridad Administrativa Competente, previo cumplimiento de las exigencias establecidas en la Ley, en su Reglamento y en las disposiciones dictadas por ella, faculta a las entidades solicitantes reguladas en el Reglamento a prestar los servicios solicitados en el marco de la Infraestructura Oficial de Firma Electrónica. |
| Agente automatizado | Procesos y equipos programados para atender requerimientos predefinidos y dar una respuesta automática sin intervención humana. |
| Autoridad Administrativa Competente - AAC | Organismo público responsable de acreditar a los Prestadores de Servicios de Certificación, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura y las otras funciones señaladas en el Reglamento o aquellas que requiera en el transcurso de sus operaciones. Dicha responsabilidad recae en el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI. |

| | |
|---|---|
| Certificado digital | Documento electrónico generado y firmado digitalmente por una entidad de certificación el cual vincula un par de claves con una persona natural o jurídica confirmando su identidad. |
| Infraestructura Oficial de Firma Electrónica - IOFE | Sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, provisto de instrumentos legales y técnicos que permiten generar firmas electrónicas y proporcionar diversos niveles de seguridad respecto a: 1) la integridad de los mensajes de datos y documentos electrónicos; 2) la identidad de su autor, lo que es regulado conforme a la Ley. El sistema incluye la generación de firmas electrónicas, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la Autoridad Administrativa Competente, incluyendo a la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), las Entidades de Certificación para el Estado Peruano (ECEP) y las Entidades de Registro o Verificación para el Estado Peruano (EREP). |
| Titular de certificado digital | Persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital. |
| Suscriptor o titular de la firma digital | Persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un mensaje de datos firmado digitalmente utilizando su clave privada. En el caso que el titular del certificado sea una persona natural, sobre la misma recaerá la responsabilidad de suscriptor. En el caso que una persona jurídica sea el titular de un certificado, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica, la cual deberá ser dueña del agente automatizado. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital. |
| Tercero que confía o tercer usuario | Personas naturales, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado y/o verifica alguna firma digital en la que se utilizó dicho certificado. |
| WebTrust for CA | Certificación otorgada a prestadores de servicios de certificación digital - PSC, específicamente a las Entidades Certificadoras - EC, que de manera consistente cumplen con estándares establecidos por el Instituto Canadiense de Contadores Colegiados (CICA por sus siglas en inglés - ver Cica.ca) y el Instituto Americano de Contadores Públicos Colegiados (AICPA).<br>Los estándares mencionados se refieren a áreas como privacidad, seguridad, integridad de las transacciones, disponibilidad, confidencialidad y no repudio. |

# 4. PARTICIPANTES

## 4.1. ENTIDAD DE CERTIFICACIÓN

SoftNet, en su papel de Entidad de Certificación, es una persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital.

### 4.2. ENTIDAD DE REGISTRO O VERIFICACIÓN

SoftNet, en su papel de Entidad de Registro o Verificación, es una persona jurídica encargada del levantamiento de datos, comprobación de éstos respecto a un solicitante de un mecanismo de firma electrónica o certificación digital, la aceptación y autorización de las solicitudes para la emisión de un mecanismo de firma electrónica o certificados digitales, así como de la aceptación y autorización de las solicitudes de cancelación de mecanismos de firma electrónica o certificados digitales.

### 4.3. PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL

emSign PKI, como parte de eMudhra, es el proveedor de servicios de certificación digital para la Entidad de Certificación de SoftNet, la cual presta su infraestructura y servicios tecnológicos a esta entidad de certificación y garantiza la continuidad del servicio a los titulares y suscriptores durante todo el tiempo en que se hayan contratado los servicios de certificación digital.

### 4.4. TITULAR

Persona natural o jurídica a cuyo nombre se expide un certificado digital y por tanto actúa como responsable de éste, confiando en él, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en la DPC de la EC de SoftNet.

### 4.5. SUSCRIPTOR

Persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un mensaje de datos firmado digitalmente utilizando su clave privada. En el caso que el titular del certificado sea una persona natural, sobre la misma recaerá la responsabilidad de suscriptor. En el caso que una persona jurídica sea el titular de un certificado, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica, la cual deberá ser dueña del agente automatizado. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

### 4.6. TERCERO QUE CONFÍA

Personas naturales, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado y/o verifica alguna firma digital en la que se utilizó dicho certificado.

## 5. SERVICIOS DE CERTIFICACIÓN DIGITAL

SoftNet brinda los servicios de emisión, re-emisión, revocación y distribución de certificados digitales, conforme a la Guía de Acreditación de Entidades de Certificación del INDECOPI
SoftNet establece la Política de Seguridad que eMudhra, como su proveedor de servicios de certificación digital, debe cumplir. En caso de incidentes que puedan afectar la seguridad de los servicios contratados a SoftNet, las responsabilidades contractuales, garantías financieras y coberturas de seguros son brindadas por ésta, de acuerdo con su documento Declaración de Prácticas de Certificación y Política de Certificación, publicado en:

http://www.soft-net.com.pe/

Los certificados y las prácticas relacionadas a la gestión de su ciclo de vida son descritos en la Declaración de Prácticas y la Política de Certificación (CP y CPS) de emSign

https://repository.emsign.com/

Los servicios de certificación digital de SoftNet serán brindados según los esquemas brindados a continuación:

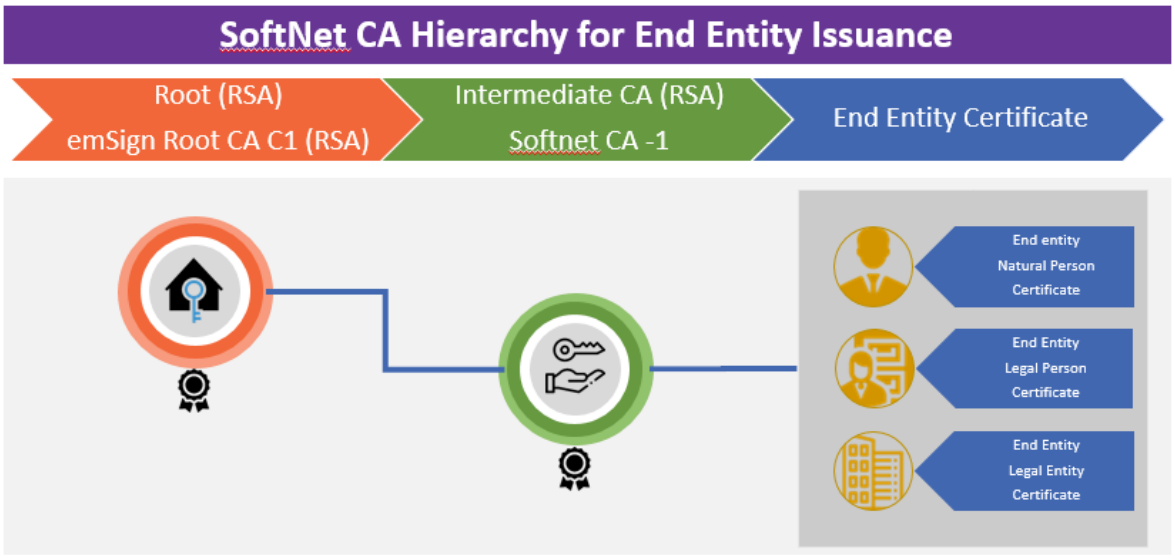



Figura 1. Jerarquía para la emisión de certificados bajo la EC se SoftNet.

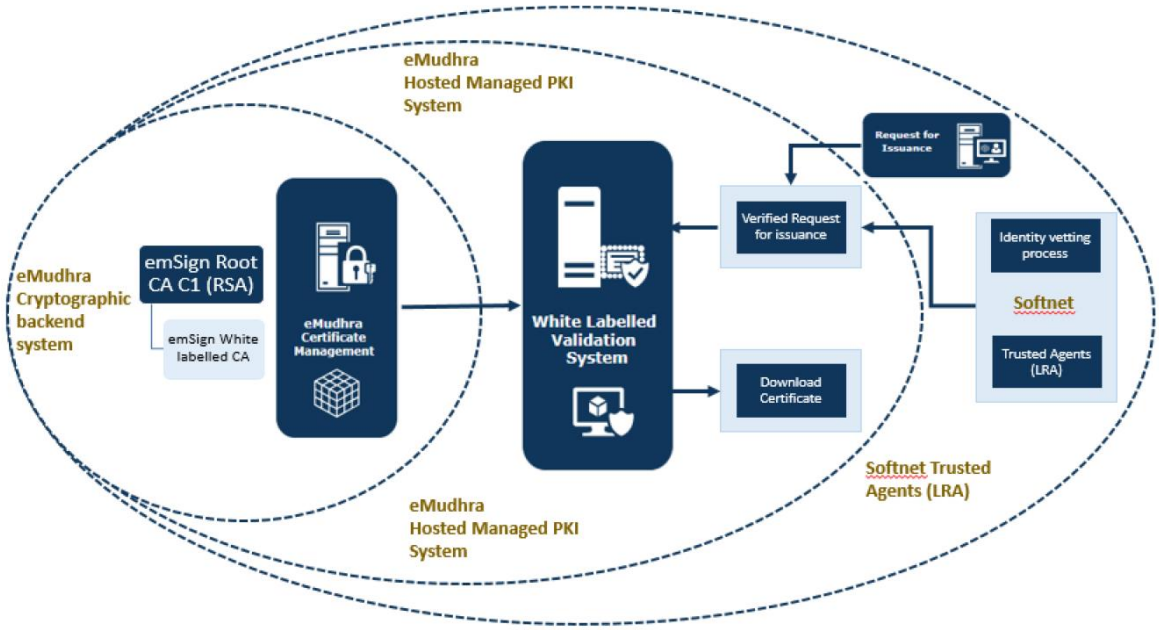



Figura 2. Flujo para la emisión de certificados AATL y/o S/MIME.

## 5.1. TIPOS DE CERTIFICADO

El OID para políticas de certificado bajo emSign PKI es:

un iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) eMudhra Technologies Limited (50977) emSign PKI (1) Certificate Type (2).

Los tipos de certificados que emite SoftNet son identificados por un OID de emSign PKI como sigue:

| **Tipo de Certificado** | **OID de la política** |
|---|---|
| Device Certificate | 1.3.6.1.4.1.50977.1.2.300 |
| Client Certificates - Class 1 | 1.3.6.1.4.1.50977.1.2.400 |
| Client Certificates - Class 2 | 1.3.6.1.4.1.50977.1.2.410 |
| Client Certificates - Class 3 | 1.3.6.1.4.1.50977.1.2.420 |
| Time Stamping Certificate | 1.3.6.1.4.1.50977.1.2.500 |
| OCSP Certificate | 1.3.6.1.4.1.50977.1.2.600 |

La CP / CPS de emSign se aplica a cualquier entidad que afirme uno o más de los OID de emSign identificados anteriormente. Cuando una EC como SoftNet emite un Certificado que contiene uno de los identificadores de política especificados anteriormente, afirma que el Certificado fue emitido y se administra de acuerdo con los requisitos aplicables a esa política respectiva.

Las revisiones posteriores a este CP pueden contener nuevas asignaciones de OID para los tipos de certificados identificados anteriormente, o pueden modificarse con nuevos tipos de certificados con los nuevos OID correspondientes.

# 6. RESPONSABILIDADES DE SOFTNET

Las responsabilidades contractuales, garantías financieras y coberturas de seguros son brindadas por SoftNet. SoftNet representa a eMudhra para todos los aspectos de mediación entre las personas naturales y jurídicas del Estado Peruano y la Entidad de Certificación emSign de eMudhra.

Asimismo, SoftNet brinda los servicios de registro o verificación conforme a las Guías de Acreditación de Entidades de Registro del INDECOPI, para realizar la verificación de identidad de las personas jurídicas y naturales solicitantes de los certificados digitales.

Las peticiones, quejas o reclamos sobre los servicios prestados por SoftNet, a través de su proveedor de servicios de certificación, emSign, deben ser enviadas a SoftNet. Los canales de atención son indicados en la sección Persona de contacto del presente documento.

La Entidad de Certificación de SoftNet es operada por emSign PKI. Debe actuar de acuerdo con su respectivos Acuerdo de CA emisora y estar sujetos a los términos de la CP / CPS de emSign. La EC de SoftNet está autorizada a emitir y administrar todos los tipos de Certificados Digitales admitidos por este CP / CPS y que son descritos en el presente documento.

Las obligaciones de las CA dentro de la PKI de emSign incluyen:

- Generar, emitir y distribuir certificados de clave pública.
- Generar y publicar información del estado del certificado (como CRL).
- Mantener la seguridad, disponibilidad y continuidad de la emisión del certificado y la CRL
- Proporcionar un medio para que los Suscriptores soliciten la revocación
- Revocación de certificados de clave pública
- Pasar por auditorías internas y externas del cumplimiento de la CP / CPS de emSign.

# 7. RESPONSABILIDADES Y OBLIGACIONES DE LOS TITULARES Y SUSCRIPTORES

Los usuarios y solicitantes de los certificados digitales provistos por SoftNet, son responsables de revisar la presente Declaración de Prácticas y Política de Certificación, a fin de conocer las características de la plataforma de servicios, infraestructura y procedimientos empleados en la gestión del ciclo de vida de los certificados digitales, Raíz, Intermedios y de usuario final, así como las obligaciones de cada parte.
Las obligaciones de los titulares y suscriptores incluyen:

- Generar o hacer que se generen uno o más pares de claves asimétricas.
- Enviar claves públicas y credenciales para el registro.
- Proporcionar información a la Entidad de Registro que sea precisa y completa respecto a la información de identificación de los titulares o suscriptores en sus certificados.
- Tomar las medidas apropiadas para proteger sus claves privadas del compromiso.
- Informar rápidamente la pérdida o el compromiso de la(s) clave(s) privada(s) y la inexactitud de la información del certificado a la Entidad de Registro o a la Entidad de Certificación.
- Utilizar en todo momento el Certificado digital de acuerdo con todas las leyes y regulaciones aplicables.
- Utilizar los pares de claves de firma para las firmas electrónicas de acuerdo con el perfil del Certificado digital y cualquier otra limitación conocida, o que deba conocerse, para el Titular del certificado.
- Suspender el uso del par de claves de firma digital en el caso de que la Entidad de Certificación emisora notifique al Titular del certificado que la Entidad de Certificación emisora se ha visto comprometida.
- Usar su(s) par(es) clave(s) de conformidad con esta Declaración de Prácticas y Política de Certificación.
- Cualquier otro término según el Acuerdo del suscriptor

# 8. USO DEL CERTIFICADO

Un certificado digital permite a las personas o entidades demostrar su identidad en transacciones electrónicas a otros participantes en dichas transacciones.

## 8.1. USO PERMITIDO DEL CERTIFICADO

Los certificados emitidos bajo esta PC y DPC se pueden usar según lo definido por las extensiones de certificado en el uso de claves y uso extendido. El alcance del uso de los certificados incluye toda autenticación legal, encriptación, control de acceso y firma. Esto es:
**Identificación del Titular**. El titular del certificado puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el certificado.
**Integridad del documento firmado**. La utilización del certificado garantiza que el documento firmado es integro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el titular. Se certifica que el mensaje recibido por el receptor o destinatario que confía es el mismo que fue emitido por el titular.
**No repudio de origen**. Con el uso de este certificado también se garantiza que la persona que firma el documento no puede repudiarlo, es decir, el Titular que ha firmado no puede negar la autoría o la integridad del mismo
autoría o la integridad del mismo.
**Sellado de Tiempo**. Es un certificado que se emite para la firma de evidencias digitales de tiempo electrónico. El sello de tiempo indica que un documento existió en un determinado instante de tiempo y que no ha sido alterado desde entonces.

### 8.2. USO PROHIBIDO DEL CERTIFICADO

Los certificados sólo podrán ser empleados para los usos para los que hayan sido emitidos y especificados en esta CPS y concretamente en las Políticas de Certificación.
Se consideran indebidos aquellos usos que no están definidos en esta CPS y en consecuencia para efectos legales, SoftNet queda eximida de toda responsabilidad por el empleo de los certificados en operaciones que estén fuera de los límites y condiciones establecidas para el uso de certificados digitales según esta CPS.

## 9. PERSONA DE CONTACTO

**Datos de la Entidad de Certificación Digital y de Registro:**
Nombre: SOFT & NET SOLUTIONS S.A.C.
Dirección: Calle German Schreiber Nro. 184 Dpto. 802
Teléfono: +511 421 2777
email: informes@soft-net.com.pe
website: www.soft-net.com.pe/

**Datos del Proveedor de Servicios de Certificación Digital:**
Nombre: emSign PKI Policy Authority eMudhra Technologies Limited (eMudhra Group Company)
Dirección: 3rd Floor, Sai Arcade, Outer Ring Road, Devarabeesanahalli, Bangalore - 560103, Karnataka, India
Teléfono: +91 80 42275300
email: info@emsign.com
website: www.emsign.com

## 10. ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS NORMATIVOS

SoftNet administra todos los documentos normativos de su EC, en particular la Política de Certificación y Declaración de Prácticas.
Para cualquier consulta contactar con:
Nombre: Leonel José García Jáuregui
Cargo: Director Comercial y de Negocios
Dirección de correo electrónico: LGARCIA@SOFT-NET.COM.PE

## 11. PUBLICACIÓN DE LOS DOCUMENTOS NORMATIVOS

La Política de Certificación y Declaración de Prácticas, la Política y Plan de Privacidad, la Política de la Seguridad de la Información de la EC de SoftNet y otra documentación relevante son publicados en la siguiente dirección: http://www.soft-net.com.pe/politicas/
Todas las modificaciones relevantes serán comunicadas al INDECOPI y las nuevas versiones del documento serán publicadas en el mismo sitio web.
El presente documento es firmado por el Responsable de la EC de SoftNet antes de ser publicado, y se controlan las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas.
Los documentos referidos a la CP/CPS de emSign PKI también estarán dsponibles desde la dirección indicada.

# 12. RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

**Certificado de Entidad de Certificación Raíz de emSign**
https://repository.emsign.com/

**Certificado de Entidad de Certificación Subordinada de SoftNet**
https://repository.emsign.com/
http://www.soft-net.com.pe/politicas/

**PC y DPC**
SoftNet
http://www.soft-net.com.pe/politicas/
emSign
https://repository.emsign.com/

## 12.1. PUBLICACIÓN DE LA INFORMACIÓN DE CERTIFICACIÓN

El Responsable de la EC de SoftNet es el encargado de la autorización de la publicación de la PC y DPC y es responsable de asegurar la integridad y disponibilidad de la información publicada en la página web: http://www.soft-net.com.pe/

## 12.2. PLAZO O FRECUENCIA DE LA PUBLICACIÓN

**Certificado Raíz**
El certificado raíz se publicará y permanecerá en la página web de la Entidad de Certificación de SoftNet durante todo el tiempo en que se estén prestando servicios de certificación digital.

**Certificado Subordinada**
El certificado de la EC Subordinada se publicará y permanecerá en la página web de la Entidad de Certificación de SoftNet durante todo el tiempo en que se estén prestando servicios de certificación digital.

**Lista de Certificados Revocados (CRL)**
emSign publicará la lista de certificados revocados en los eventos y con la periodicidad definidas en el numeral Frecuencia de emisión de las CRLs.

**Declaración de Prácticas de Certificación (CPS)**
Con autorización del Responsable de la Entidad de Certificación de SoftNet y el INDECOPI, se publicará la versión finalmente aprobada. Los cambios generados en cada nueva versión serán previamente informados al INDECOPI y publicados en la página web de la Entidad de Certificación de SoftNet junto con la nueva versión. La auditoría anual validará estos cambios y emitirá el informe de cumplimiento.

**Validación de Certificados**
La Entidad de Certificación de SoftNet publica los certificados emitidos en un repositorio en formato X.509 V3.

### 12.3. CONTROLES DE ACCESO A LOS REPOSITORIOS

La consulta a los repositorios disponibles en la página web de emSign, antes mencionados, es de libre acceso al público en general. La integridad y disponibilidad de la información publicada es responsabilidad de emSign, que cuenta con los recursos y procedimientos necesarios para restringir el acceso a los repositorios con otros fines diferentes a la consulta y a la página Web por parte de personas ajenas a emSign.

## 13. IDENTIFICACIÓN Y AUTENTICACIÓN

La ER de SoftNet s CA o aquellas ER acreditadas asociadas por contrato o convenio con la EC de SoftNet, pueden realizar la Identificación y Autenticación requerida en relación con la emisión de Certificados Digitales. El nivel de Identificación y Autenticación depende de la clase y / o tipo de Certificado Digital que se emite y esto puede incluir la verificación de identidad presencial / video / biométrica al comienzo del procedimiento de solicitud de Certificado Digital o en algún momento antes de la entrega del certificado digital al Titular del Certificado.

### 13.1. NOMBRES

#### 13.1.1. TIPOS DE NOMBRES

Todos los nombres emitidos por emSign PKI cumplen con los estándares de nombres distinguidos X.500. Cada certificado de firma digital deberá contener un nombre distinguido X.501 en el campo Nombre del sujeto. Los certificados digitales emitidos por emSign PKI utilizarán nombres distinguidos (DN) para facilitar la identificación de los suscriptores. El Nombre distinguido puede formar parte de los campos según lo requiera el Perfil de certificado del tipo y / o clase respectivos del certificado.

##### 13.1.1.1. CERTIFICADO RAÍZ DE EMSIGN

El DN del “issuer name” del certificado raíz tiene los siguientes campos y valores fijos:
CN = emSign Root CA - C1
O = eMudhra Inc
OU = emSign PKI
C = US

El DN del “subject name” del certificado raíz tiene los siguientes campos y valores fijos:
CN = emSign Root CA - C1
O = eMudhra Inc
OU = emSign PKI
C = US

##### 13.1.1.2. CERTIFICADO DE LA SUBORDINADA SOFTNET

El DN del “issuer name” del certificado de la subordinada tiene los siguientes campos y valores fijos:
CN = emSign Root CA - C1
O = eMudhra Inc
OU = emSign PKI
C = US

El DN del "subject name" del certificado de la subordinada tiene los siguientes campos y valores fijos:
CN = Soft-Net Secure Signing CA - C1
O = Soft and Net Solutions SAC
OU = emSign PKI
C = PE

#### 13.1.1.3. CERTIFICADO DE TSA RAIZ DE EMSIGN

El DN del "issuer name" del certificado de TSA raíz tiene los siguientes campos y valores fijos:
CN = emSign Root CA - C1
O = eMudhra Inc
OU = emSign PKI
C = US

El DN del "subject name" del certificado de TSA raíz tiene los siguientes campos y valores fijos:
CN = emSign Time Stamping CA - C1
O = eMudhra Inc
OU = emSign PKI
C = US

#### 13.1.1.4. CERTIFICADO DE TSU DE SOFTNET

El DN del "issuer name" del certificado de TSU tiene los siguientes campos y valores fijos:
CN = emSign Root CA - C1
O = eMudhra Inc
OU = emSign PKI
C = US

El DN del "subject name" del certificado de TSU tiene los siguientes campos y valores fijos:
CN=Soft-Net Timestamping Responder
OU=emSign PKI
O=Soft and Net Solutions SAC
C=PE

### 13.1.2. NECESIDAD DE QUE LOS NOMBRES TENGAN SIGNIFICADO

Los nombres distintivos (DN) de los certificados emitidos por emSign, como prestador de servicios de SoftNet, deben tener significado y la identificación de los atributos asociados al Suscriptor debe encontrase de forma legible para humanos.

### 13.1.3. ANONIMATO Y SEUDOANONIMATO DE LOS TITULARES

No se podrán utilizar alias en los campos de Titular ya que dentro del certificado debe figurar el verdadero nombre, razón social sigla y/o denominación del solicitante del certificado.

### 13.1.4. REGLAS PARA LA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRE

La regla utilizada para interpretar los nombres distintivos del emisor y de los titulares de certificados que emite SoftNet es el estándar ISO/IEC 9595 (X.500) Distinguished Name (DN).

#### 13.1.5. SINGULARIDAD DE LOS NOMBRES

Los DN de los certificados emitidos es único.

#### 13.1.6. RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE MARCAS RECONOCIDAS

La EC de SoftNet no está obligada a recopilar o solicitar evidencia en relación con la posesión o titularidad de marcas registradas u otros signos distintivos antes de la emisión de los certificados. Esta política se extiende al uso y empleo de nombres de dominio.

# 14. VALIDACIÓN INICIAL DE LA IDENTIDAD

## 14.1. MÉTODO PARA DEMOSTRAR LA POSESIÓN DE LA CLAVE PRIVADA

Si el par de claves es generado por la entidad final (solicitante o futuro suscriptor), a continuación, se solicita una demostración de la posesión de la clave privada asociada a la clave pública. Los medios aceptados son la generación de una solicitud de Firma de certificado (CSR) vinculado a la clave privada, o cualquier otro método aceptado por emSign.
Si el par de claves es generado por la EC o la ER, emSign define y hace cumplir procedimientos aprobados para transferir de forma segura la clave privada para el suscriptor (es decir, enviar archivos PFX y contraseñas por diferentes canales y eliminar cualquier clave privada de firma una vez que la transferencia es efectiva).

## 14.2. AUTENTICACIÓN DE LA IDENTIDAD DE UNA ORGANIZACIÓN (PERSONA JURÍDICA)

Los procedimientos de autenticación de la identidad de personas jurídicas son descritos en el documento de Declaración de Prácticas de Registro o Verificación de la ER de SoftNet, u otra ER acreditada por INDECOPI y autorizada por SoftNet.
No obstante lo anterior, SoftNet y emSign se reservan el derecho de no expedir certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial y/o idoneidad legal o moral de todo el sistema de certificación.

## 14.3. AUTENTICACIÓN DE UNA IDENTIDAD INDIVIDUAL (PERSONA NATURAL)

Los procedimientos de autenticación de la identidad de los titulares y suscriptores son descritos en el documento de Declaración de Prácticas de Registro o Verificación de la ER de SoftNet, u otra ER acreditada por INDECOPI y autorizada por SoftNet.
No obstante lo anterior, SoftNet y emSign, se reservan el derecho de no expedir certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial y/o idoneidad legal o moral de todo el sistema de certificación.

## 14.4. AUTENTICACIÓN DE LA IDENTIDAD DE SISTEMAS DE INFORMACIÓN

Los procedimientos de autenticación de la identidad de sistemas de información son descritos en el documento de Declaración de Prácticas de Registro o Verificación de la ER de SoftNet, u otra ER acreditada por INDECOPI y autorizada por SoftNet.
No obstante lo anterior, SoftNet y emSign, se reservan el derecho de no expedir certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial y/o idoneidad legal o moral de todo el sistema de certificación.

### 14.5. INFORMACIÓN DE TITULAR NO VERIFICADA

Bajo ninguna circunstancia SoftNet omitirá las labores de verificación que conduzcan a la identificación del Titular y que se traduce en la solicitud de exhibición de los documentos mencionados para organizaciones y personas naturales.

### 14.6. VALIDACIÓN DE LA AUTORIDAD

Los procedimientos de autenticación de validación son descritos en el documento de Declaración de Prácticas de Registro o Verificación de la ER de SoftNet, u otra ER acreditada por INDECOPI y autorizada por SoftNet.

### 14.7. CRITERIOS PARA LA INTEROPERABILIDAD

emSign, como prestador de servicios de certificación de SoftNet, únicamente emitirá certificados a EC Subordinadas, que estén directamente vinculadas y operadas por emSign.

## 15. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RE-EMISIÓN DE CLAVES

Para los certificados de CA, la renovación del certificado se permite por medio de un nuevo certificado con un período de validez extendido para un Distinguished Name existente.
Para los Certificados de Suscriptor, la renovación se permite mediante la reutilización de una solicitud de certificado anterior para reemplazar un certificado que aun no ha vencido. Mientras el certificado no esté revocado, emSign PKI puede autenticar una solicitud de certificado de renovación utilizando una frase de contraseña o cualquier tipo de secreto compartido o cualquier otra forma de mecanismo de autenticación de suscriptor.

### 15.1. IDENTIFICACIÓN Y AUTENTICACIÓN PARA RE-EMISIÓN DE RUTINA

Para entidades emisoras, emSign no admite la renovación de claves o renovaciones automatizadas. La entidad solicitante debe seguir una ceremonia formal de creación de clave de la EC y un oficial designado apropiadamente debe verificar que la información contenida en el certificado de EC es válida.
Para los certificados de entidad final gestionados mediante una interfaz de ER aplicado o proporcionado por emSign, el suscriptor o un Oficial de registro autorizado puede utilizar sus credenciales de acceso para iniciar y aprobar, respectivamente, un certificado de cambio de la clave o re-emisión.

### 15.2. IDENTIFICACIÓN Y AUTENTICACIÓN TRAS UNA REVOCACIÓN

emSign, como prestador de servicios de SofNet, no admite la renovación de clave de los certificados después de una revocación. El suscriptor debe solicitar un nuevo certificado digital mediante el uso de los procedimientos para su emisión.

## 16. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

La política de identificación para las solicitudes de revocación es la misma que se estipula para el registro inicial. Las solicitudes telemáticas sólo serán aceptadas si estas incluyen una firma digital utilizando el certificado del suscriptor que solicitó la revocación, o el certificado de un tercero que está autorizado a solicitar la revocación en nombre del suscriptor.

Una Entidad de Certificación puede definir, que durante el proceso de inscripción, un suscriptor puede crear una contraseña que se puede utilizar en las solicitudes de revocación remotas, utilizando un procedimiento online comunicado al usuario cuando se expide el certificado.
emSign, como prestador de servicios de certificación de SotNet, puede solicitar la revocación de un certificado si hay conocimiento o sospecha fundada de que la clave privada asociada ha sido comprometida, o razones para creer cualquier otro dato que recomienda esta acción.

# 17. REQUISITOS OPERACIONALES PARA EL TIEMPO DE VIDA DE LOS CERTIFICADOS

## 17.1. SOLICITUD DEL CERTIFICADO

Las Entidades de registro que operan bajo SoftNet son las competentes y responsables de determinar si el tipo de certificado solicitado es adecuado para el solicitante y futuro suscriptor, de conformidad con la Política de Certificación en relación con dicho certificado, y por lo tanto proceder o no con la emisión del certificado.

## 17.2. QUIÉN PUEDE SOLICITAR UN CERTIFICADO

Una solicitud de certificado puede ser presentada por el titular del certificado o por un representante autorizado por él. Esto es, toda persona natural o jurídica legalmente facultada y debidamente identificada puede tramitar la solicitud de emisión de un certificado digital.

- La solicitud en el caso de personas naturales debe ser hecha por la misma persona que pretende ser titular del certificado o por un representante que cuente con facultades expresas para tales efectos otorgadas mediante poder. En este caso, el titular del certificado será el poderdante y corresponderá al apoderado la condición de suscriptor. El ámbito de utilización del certificado digital en este supuesto se encontrará circunscrito y limitado a las facultades expresamente conferidas en el poder.
- En el caso de personas jurídicas, se pueden solicitar certificados de atributo para ser usados por funcionarios y personal específico, incluso por el Representante legal. En este caso, se considera como aspirante a titular del certificado a la persona jurídica y dichas personas naturales vienen a ser los aspirantes a ser suscriptores. En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por un representante designado por la persona jurídica dueña del dispositivo. En este caso, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

Los procedimientos de solicitud según el tipo de titular son descritos en el documento de Declaración de Prácticas de Registro o Verificación de la ER de SoftNet, u otra ER acreditada por INDECOPI y autorizada por SoftNet.

## 17.3. PROCESO DE REGISTRO Y RESPONSABILIDADES

El proceso de registro, incluyendo la información verificada y las atribuciones para ejecutar el proceso se detalla en la Declaración de Prácticas de Registro o Verificación de la ER de SoftNet, u otra ER acreditada por INDECOPI y autorizada por SoftNet.

# 18. TRAMITACIÓN DE SOLICITUD DE CERTIFICADOS

## 18.1. REALIZACIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Este proceso se detalla en la Declaración de Prácticas de Registro o Verificación de la ER de SoftNet, u otra ER acreditada por INDECOPI y autorizada por SoftNet.

## 18.2. APROBACIÓN O RECHAZO DE LAS SOLICITUDES DE CERTIFICADO

Este proceso se detalla en la Declaración de Prácticas de Registro o Verificación de la ER de SoftNet, u otra ER acreditada por INDECOPI y autorizada por SoftNet.

## 18.3. PLAZO PARA PROCESAR LAS SOLICITUDES DE CERTIFICADO

Este proceso se detalla en la Declaración de Prácticas de Registro o Verificación de la ER de SoftNet, u otra ER acreditada por INDECOPI y autorizada por SoftNet.

# 19. EMISIÓN DE CERTIFICADOS

## 19.1. ACTUACIONES DE LA EC DURANTE LA EMISIÓN DE CERTIFICADOS

Una Entidad de certificación adherida a emSign procede a emitir un certificado solo después de la ejecución de las medidas necesarias para verificar que la petición recibida por una Entidad de Registro es genuina. Los controles específicos están estipulados en la Política de Certificación correspondiente.

## 19.2. NOTIFICACIÓN AL SOLICITANTE POR LA EC DE LA EMISIÓN DEL CERTIFICADO

Después de ser emitido un certificado, la EC notifica a la ER de la emisión y la disponibilidad del certificado, y el nuevo certificado se publica en el repositorio de certificados.
El mecanismo de notificación puede ser acordado específicamente con el suscriptor. En general, para los certificados personales, la ER es responsable de notificar al suscriptor de la disponibilidad de su certificado, enviándole una copia o mediante la especificación de cómo se puede obtener el certificado.
Las notificaciones electrónicas pueden ser firmadas digitalmente por la ER o representante habilitado.

# 20. ACEPTACIÓN DEL CERTIFICADO

## 20.1. FORMA EN LA QUE SE ACEPTA EL CERTIFICADO

La aceptación del certificado queda entendida después de que el suscriptor o su representante lleva a cabo uno o más de los siguientes puntos:

- Se firma el "Acuerdo del suscriptor o titular", que incluye los términos y condiciones asociadas con la política de certificado, y que constituye la aceptación formal de los términos.
- Se descarga y/o instala el certificado, por lo que es técnicamente disponible para el uso.
- No se rechaza explícitamente el certificado una vez que la disponibilidad de la notificación ha sido enviada.

### 20.2. PUBLICACIÓN DEL CERTIFICADO POR LA EC

Las entidades emisoras que operan bajo emSign publican todos los certificados emitidos.

### 20.3. NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA EC A OTRAS ENTIDADES

No aplica.

## 21. USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO

### 21.1. USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL TITULAR

Los usos específicos permitidos para una clave privada asociada a un tipo de certificado emitido por SoftNet a través de emSign son tal y como se detalla en la sección Uso permitido del certificado del presente documento.

### 21.2. USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR TERCEROS QUE CONFÍAN

El tercero que confía debe acceder y utilizar la clave pública y certificado conforme a lo estipulado en la presente PC y DPC y tal como se indica en el documento "Acuerdo del tercero que confía", hecho público en la página web de SoftNet.

## 22. RE-EMISIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES

### 22.1. CIRCUNSTANCIAS PARA LA RE-EMISIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

Un certificado solo se puede re-emitir para los certificados personales y corporativos que siguen siendo válidos y de próxima expiración. La renovación de los certificados caducados no es compatible con esta PCy DPC.

### 22.2. QUIÉN PUEDE SOLICITAR UNA RE-EMISIÓN CON CAMBIO DE CLAVES

La re-emisión del certificado puede ser solicitado por las mismas entidades autorizadas para solicitar la primera emisión del certificado.

### 22.3. TRÁMITES PARA LA SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

La solicitud de re-emisón del certificado será procesada por el correspondiente Oficial de Registro, verificando que ninguno de los atributos del nuevo certificado se haya cambiado en los últimos treinta y nueve (39) meses, de acuerdo con los Requisitos base. Cualquier cambio en un atributo será convenientemente validado, tal como se define en las secciones pertinentes de la presente PC y DPC.

### 22.4. NOTIFICACIÓN AL TITULAR DE LA EMISIÓN DE UN NUEVO CERTIFICADO CON CAMBIO DE CLAVES

La notificación de la emisión de un certificado re-emitido se producirá como se describe en la sección Notificación al solicitante por la EC de la emisión del certificado de este documento.

### 22.5. FORMA EN LA QUE SE ACEPTA LA RE-EMISIÓN DE UN CERTIFICADO

Como se estipula en la sección Forma en la que se acepta el certificado de este documento.

### 22.6. PUBLICACIÓN DEL CERTIFICADO RE-EMITIDO POR LA EC

Como se estipula en la sección Publicación del certificado por la EC de este documento.

### 22.7. NOTIFICACIÓN DE LA EMISIÓN DE UN CERTIFICADO RE-EMITIDO POR LA EC A OTRAS ENTIDADES

Como se indica en la sección Notificación al solicitante por la EC de la emisión del certificado, la EC solo notifica a la ER del que haya recibido la solicitud de la emisión de un certificado. Es deber de la ER notificar al suscriptor del certificado.

## 23. RE-EMISIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVES

### 23.1. CIRCUNSTANCIAS PARA LA RE-EMISIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES

emSIgn, como prestador de servicios de certificación de SoftNet, no realiza la re-emisión de certificados sin cambio de claves.

### 23.2. QUIÉN PUEDE SOLICITAR UNA RE-EMISIÓN SIN CAMBIO DE CLAVES

emSIgn, como prestador de servicios de certificación de SoftNet, no realiza la re-emisión de certificados sin cambio de claves.

### 23.3. TRÁMITES PARA LA SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES

emSIgn, como prestador de servicios de certificación de SoftNet, no realiza la re-emisión de certificados sin cambio de claves.

### 23.4. NOTIFICACIÓN AL TITULAR DE LA EMISIÓN DE UN NUEVO CERTIFICADO SIN CAMBIO DE CLAVES

emSIgn, como prestador de servicios de certificación de SoftNet, no realiza la re-emisión de certificados sin cambio de claves.

### 23.5. FORMA EN LA QUE SE ACEPTA LA RE-EMISIÓN DE UN CERTIFICADO

emSIgn, como prestador de servicios de certificación de SoftNet, no realiza la re-emisión de certificados sin cambio de claves.

### 23.6. PUBLICACIÓN DEL CERTIFICADO RE-EMITIDO POR LA EC

emSIgn, como prestador de servicios de certificación de SoftNet, no realiza la re-emisión de certificados sin cambio de claves.

### 23.7. NOTIFICACIÓN DE LA EMISIÓN DE UN CERTIFICADO REEMITIDO POR LA EC A OTRAS ENTIDADES

emSIgn, como prestador de servicios de certificación de SoftNet, no realiza la re-emisión de certificados sin cambio de claves.

## 24. MODIFICACIÓN DE CERTIFICADOS

emSIgn, como prestador de servicios de certificación de SoftNet, no permite la modificación de los certificados durante su periodo de validez. Si la información contenida en un certificado deja de ser válido, o las circunstancias del suscriptor cambian de manera tal que las condiciones expresadas en la PC y DPC no se cumplen, entonces el único procedimiento aceptado es la revocación y re-emisión de un nuevo certificado.

## 25. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

### 25.1. CIRCUNSTANCIAS PARA LA REVOCACIÓN DE UN CERTIFICADO

La EC que opere bajo emSign debe revocar un certificado que ha emitido, sobre la ocurrencia de cualquiera de los siguientes eventos:

1. El suscriptor solicita la revocación de su certificado.
2. El suscriptor indica que el certificado original no estaba autorizado y no le concede retroactivamente la autorización.
3. La EC obtiene evidencia razonable de que la clave privada del suscriptor (correspondiente a la clave pública en el certificado) ha sido comprometida o se sospecha de compromiso, o de lo contrario el certificado ha sido mal utilizado.
4. La EC recibe aviso o caso contrario se da cuenta de que un suscriptor ha violado una o más de sus obligaciones fundamentales bajo el contrato de suscriptor o condiciones de uso.
5. La EC recibe aviso o caso contrario se da cuenta de que un tribunal o árbitro ha revocado el derecho de un suscriptor para utilizar un nombre (por ejemplo, un nombre de dominio) que aparece en el certificado, o que el suscriptor no ha logrado renovar su derecho a utilizar ese nombre.
6. La EC recibe aviso o de lo contrario se da cuenta de un cambio sustancial en la información contenida en el certificado.
7. Una determinación, a la sola discreción de la autoridad competente, de que el certificado no ha sido emitido de conformidad con los términos y condiciones derivadas de la política de certificación apropiada
8. La EC determina que alguna de la información que aparece en el certificado no es exacta.
9. La EC cesa su actividad por cualquier razón y no ha dispuesto otra EC bajo emSign PKI para proporcionar soporte de revocación del certificado.
10. El derecho de la EC de emitir certificados para una política de certificado expira o es revocado o terminado, a menos que la EC haga los arreglos para seguir manteniendo el repositorio CRL/OCSP.
11. La clave privada de cualquier EC en el curso de certificación se sospecha que ha sido comprometida.

12. El suscriptor es un participante en el PKI (por ejemplo, Registro Oficial) y pierde su derecho de acceso para seguir actuando como tal.
13. La EC recibe aviso o de lo contrario se da cuenta de que un suscriptor se ha añadido como una parte denegada o persona prohibida de una lista negra, o está operando desde un lugar o de una manera que está prohibida en virtud de las leyes y la jurisdicción del país de operación de la EC.

## 25.2. QUIÉN PUEDE SOLICITAR UNA REVOCACIÓN

El suscriptor o representante legal pueden solicitar la revocación de un certificado individual u organizacional.
La ER autorizada o representante titulado pueden solicitar la revocación de un certificado si se presenta alguna de las circunstancias expresadas en el apartado anterior.

## 25.3. PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN

El procedimiento que se utiliza para las solicitudes de revocación de certificados se detalla en el "Contrato de titular/suscriptor".
Los usuarios individuales podrán encontrar el contacto adecuado e información del procedimiento en el URL http://www.soft-net.com.pe/politicas/
La práctica común para todos los certificados emitidos por emSign es que las solicitudes de revocación sean aceptadas de forma automática y produzcan una revocación inmediata en el caso de:

- Solicitudes remotas enviadas por correo electrónico o a través de una página web o servicio, debidamente autenticados por el suscriptor o su representante.
- Las solicitudes presenciales dirigidas a un representante de la ER y la identidad del solicitante se demuestra por el mismo medio que el utilizado para el registro de certificados.
- Las solicitudes de revocación enviados por un representante oficial de registro o certificación.

## 25.4. PERIODO DE GRACIA DE SOLICITUD DE REVOCACIÓN

No se estipula un periodo de gracia para las solicitudes de revocación. El proceso de revocación se iniciará inmediatamente después de la recepción de dicha solicitud por la ER o EC.

## 25.5. PLAZO EN EL QUE LA EC DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN

Las solicitudes de revocación son procesadas por la EC en el plazo más breve posible.

## 25.6. REQUISITOS DE VERIFICACIÓN DE LAS REVOCACIONES POR LOS TERCEROS QUE CONFÍAN

Es responsabilidad del titular de un certificado digital y éste así lo acepta y reconoce, informar a los Terceros que confían de la necesidad de comprobar la validez de los certificados digitales sobre los que esté haciendo uso en un momento dado. Informará igualmente el titular al Tercero que confía que, para realizar dicha consulta, dispone de la lista de certificados revocados CRL, publicada de manera de periódica por SoftNet.

## 25.7. FRECUENCIA DE EMISIÓN DE LAS CRLs

Cada vez que se produzca una revocación de un certificado, SoftNet generará y publicará una nueva CRL de manera inmediata en su repositorio y a pesar de que no se produzca ninguna revocación cada veinticuatro (24) horas se generará y publicará una nueva CRL.

## 25.8. TIEMPO MÁXIMO DE LATENCIA DE LAS CRLs

El tiempo entre la generación y publicación de la CRL es mínimo debido a que la publicación es automática, menor a una hora como lo establece el INDECOPI.

## 25.9. REVOCACIÓN ON-LINE/DISPONIBILIDAD DE VERIFICACIÓN DEL ESTADO

emSign, como prestador de servicios de certificación de SoftNet, publicará tanto la CRL como el estado de los certificados revocados en repositorios de libre acceso y fácil consulta, con disponibilidad 7X24 durante todos los días del año.
La URL utilizada para acceder al servicio OCSP está incluido en la "extensión AIA" en todos los certificados emitidos.
Para ciertos Certificados de la EC emisora se podría publicar en servicios online, webbased u otros.

## 25.10. REQUISITOS DE COMPROBACIÓN DE LA REVOCACIÓN ONLINE

La comprobación de la revocación online se ofrece abiertamente sin restricción a todos los participantes en la PKI, para los tipos de certificados que incluyan la extensión AIA apropiado.
Se solicita a los terceros que confían verificar siempre la validez del certificado en la que se basan, según lo estipulado en el apartado Requisitos de verificación de las revocaciones por los terceros que confían.

## 25.11. OTRAS FORMAS DISPONIBLES DE DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN

No se estipula.

## 25.12. REQUISITOS ESPECIALES DE RENOVACIÓN DE CLAVES COMPROMETIDAS

Cualquier tercero que detecte un compromiso de la clave en cualquier nivel es requerido para comunicar inmediatamente esto a la Entidad de Registro o a la Entidad de Certificación.

## 25.13. CIRCUNSTANCIAS PARA LA SUSPENSIÓN

SoftNet no dispone del servicio de suspensión de certificados digitales, únicamente revocación.

## 25.14. QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

No aplica por cuanto SoftNet no dispone del servicio de suspensión de certificados digitales, únicamente revocación.

## 25.15. PROCEDIMIENTO DE SOLICITUD DE SUSPENSIÓN

No aplica por cuanto SoftNet no dispone del servicio de suspensión de certificados digitales, únicamente revocación.

## 25.16. LÍMITES DEL PERIODO DE SUSPENSIÓN

No aplica por cuanto SoftNet no dispone del servicio de suspensión de certificados digitales, únicamente revocación.

# 26. SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

## 26.1. CARACTERÍSTICAS OPERACIONALES

Los servicios de estado de certificados son accesibles a través de servidores HTTP pertenecientes a las EC de emSign. Se puede acceder a los servicios mediante la descarga de listas de revocación (CRL) o mediante el envío de solicitudes a los servidores OCSP.
Las direcciones URL de servicios de información de revocación de certificados apropiados se incluyen en las extensiones estándar dentro de los certificados emitidos.
Otros servicios podrían estar disponibles, según lo estipulado en el "Contrato de suscriptor/titular" correspondiente.

## 26.2. DISPONIBILIDAD DEL SERVICIO

El servicio de consulta del estado de certificados digitales tiene una disponibilidad 7X24 durante todos los días del año.

## 26.3. CARACTERÍSTICAS OPCIONALES

No se estipula.

## 26.4. FINALIZACIÓN DE LA VIGENCIA DE UN CERTIFICADO

La Entidad de Certificación de SoftNet da por finalizada la vigencia de un certificado digital emitido ante las siguientes circunstancias:

- Pérdida de validez por revocación del certificado digital.
- Vencimiento del periodo para el cual un titular contrato la vigencia del certificado.

# 27. CUSTODIA Y RECUPERACIÓN DE CLAVES

## 27.1. ALMACENAMIENTO DE LA CLAVE PRIVADA DEL TITULAR

La clave privada del titular se puede almacenar en un dispositivo software o hardware. El dispositivo criptográfico en hardware utilizado por SoftNet es una tarjeta criptográfica o token USB que cumple los requerimientos mínimos de la normatividad vigente y las garantías de la certificación europea Common Criteria como "dispositivo seguro de creación de firma". Estos dispositivos criptográficos seguros de creación de firma, cumplen con las certificaciones como chip criptográfico: nivel de seguridad CC EAL5+ PP 9806, BSI-PP-002- 2001, FIPS 140-2 NIVEL 3 y las certificaciones SO del chip criptográfico: nivel de seguridad CC EAL4+ BSI-PP-0006-2002 (CWA 14169 SSCD Type-3) – BSI –DSZ-CC-0422-2008 y soportan los estándares PKCS#11, Microsoft CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPsec/IKE. SoftNet publica en su portal las características de los dispositivos criptográficos que ofrece a los titulares que así lo solicitan para creación y almacenamiento de sus claves privadas.

## 27.2. PRÁCTICAS Y POLÍTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

La generación de la clave privada es responsabilidad del titular y es generada directamente sobre un dispositivo seguro (hardware), del cual no se puede exportar. En consecuencia, no es posible la recuperación de la clave privada del titular debido a que no existe copia alguna. La responsabilidad de la custodia de la clave privada es del titular y éste así lo acepta y reconoce.

### 27.3. PRÁCTICAS Y POLÍTICAS DE CUSTODIA Y RECUPERACIÓN DE LA CLAVE DE SESIÓN

La recuperación de la clave de sesión del titular o PIN, no es posible ya que no existe copia alguna por cuanto es él, el único que puede generarlo y este así lo declara y acepta. La responsabilidad de la custodia de la clave de sesión o PIN es del titular quien acepta no mantener registros digitales, escritos o en cualquier otro formato y quien se obliga a memorizarlo, por lo que su olvido requiere la solicitud de revocación del certificado y la solicitud de uno nuevo por cuenta del titular.

## 28. CONTROLES FÍSICOS DE LA INSTALACIÓN, GESTIÓN Y OPERACIONALES

emSign PKI es el proveedor de servicios de certificación digital de SoftNet, por lo cual proporciona a SoftNet su producto Enterprise Hosted Managed PKI Solution, desde su centro de datos en la India, de tal forma que es el responsable de los controles físicos, de gestión y operacionales de dichas instalaciones.

### 28.1. CONTROLES FÍSICOS DE LA INFRAESTRUCTURA TECNOLÓGICA A TRAVÉS DE LA CUAL SOFTNET PRESTA SUS SERVICIOS

emSign PKI, como proveedor de servicio de certificación de SoftNet, cuenta con controles físicos apropiados para lo siguiente:

1. Control de acceso físico al hardware utilizado en conexión con las operaciones de EC.
2. Control de acceso físico sobre el software relevante.
3. Protección contra incendios.
4. Protección contra fallas de servicios de soporte como energía, telecomunicaciones, etc.
5. Protección contra el robo.
6. Procedimientos de recuperación de desastres.

#### 28.1.1. UBICACIÓN FÍSICA Y CONSTRUCCIÓN

SoftNet realiza sus operaciones de EC desde un centro de datos seguro, el cual es proporcionado por emSign PKI en calidad de su proveedor de servicios de certificación. Dicho cenro de datos cuenta con las siguientes características:

- El centro de datos está equipado con controles físicos y lógicos que hagan que las operaciones de la EC sean inaccesibles para personas no autorizadas.
- El centro de datos es una instalación de hormigón y acero.
- El centro de datos tiene mecanismos de protección de seguridad tales como guardias, cerraduras de puertas.
- El centro de datos es de construcción de piso elevado y una serie de sistemas de seguridad y ambientales resilientes.

#### 28.1.2. ACCESO FÍSICO

La EC de SoftNet se encuentran en un centro de datos seguro proporcionado por el PSC emSign PKI. La entrada a esta instalación segura sólo se permite al personal autorizado y aquel personal autorizado por la seguridad del centro de datos, cuyos movimientos dentro de la instalación se registran y auditan. El acceso físico a esta instalación también se graba en video las 24 horas, los 7 días de la semana. El personal de seguridad in situ supervisa el acceso físico adicional a esta instalación 24/7.

### 28.1.3. ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

El suministro de energía de la EC de SoftNet, como EC emisora de los sistemas emSign PKI, está protegido con dos fuentes de alimentación mediante el uso de sistemas y generadores de suministro de energía ininterrumpida (UPS) para evitar un apagado anormal en caso de una falla de energía.
Se han implementado sistemas de control climático para garantizar que la temperatura dentro de todas las instalaciones de las EC emisoras de emSign PKI se mantenga dentro de límites operativos razonables.

### 28.1.4. EXPOSICIÓN AL AGUA

Las instalaciones de la EC de SoftNet, proporcionado por emSign, están ubicadas fuera de cualquier área propensa a inundaciones. Además, se encuentra en un piso superior con pisos elevados, que brindan protección contra la exposición al agua. Además, las paredes exteriores también están selladas para proporcionar protección contra la exposición al agua.

### 28.1.5. PREVENCIÓN Y PROTECCIÓN DE INCENDIOS

El centro de datos de emSign que aloja la EC de SoftNet, está equipado con un sistema de detección de humo. También está equipado con el sistema de extinción de incendios (FM200) y el dispositivo de detección de humo muy temprano (VESDA) necesarios para la protección contra incendios.

### 28.1.6. SISTEMA DE ALMACENAMIENTO

Todos los medios magnéticos que contienen información de la EC de SoftNet y que son administrados por eMudhra, incluidos los medios de respaldo, se almacenan en contenedores, gabinetes o cajas fuertes con capacidades de protección contra incendios. Además, se encuentran dentro del área de operaciones del servicio emSign PKI o en un área de almacenamiento segura fuera del sitio y están protegidos contra cualquier acceso físico no autorizado.

### 28.1.7. ELIMINACIÓN DEL MATERIAL DE ALMACENAMIENTO DE LA INFORMACIÓN

La EC de SoftNet, como EC emisora de emSign PKI, dispone de mecanismos de eliminación de información comercial confidencial o confidencial como se indica a continuación:

- En caso de papel u otro material impreso que contenga dicha información, se triturará o destruirá en un procedimiento generalmente aceptado.
- En el caso de medios magnéticos que contengan elementos confiables de la EC o información comercial confidencial o confidencial, se eliminará de forma segura por daño físico o destrucción completa del activo o mediante el uso de una utilidad aprobada para limpiar o sobrescribir los medios magnéticos;

### 28.1.8. BACKUP FUERA DE LA INSTALACIÓN

emSign garantiza el empleo de una ubicación fuera del sitio para el almacenamiento y la retención de software y datos de respaldo relacionados con las operaciones de la EC de SoftNet.
El almacenamiento fuera de la instalación:

- Está disponible para personal autorizado las 24 horas del día, los siete días de la semana con el fin de recuperar software y datos.
- Tiene niveles apropiados de seguridad física.
- Se almacenan en cajas fuertes y contenedores resistentes al fuego.

## 28.2. CONTROLES DE PROCEDIMIENTO

La EC de SoftNet, como EC emisora de emSign PKI, asegura que se adhiere a todos los procesos y procedimientos administrativos detallados en la CP / CPS de emSign PKI los cuales se tratan y describen en detalle en los diversos documentos utilizados dentro y que respaldan a dicho proveedor de servicios de certificación.

### 28.2.1. ROLES DE CONFIANZA

Se crean roles de confianza en el sistema emSign PKI con el fin de garantizar que una persona que actúe sola no pueda eludir las salvaguardas de seguridad implementadas en el sistema de la EC de SoftNet. Para garantizar esto, las responsabilidades son compartidas por múltiples roles e individuos. Esto se logra creando roles y cuentas separadas en varios componentes del sistema de la EC de SoftNet, y cada rol tiene una capacidad limitada. Este método permite que ocurra un sistema de "controles y equilibrios" entre los diversos roles.
Los roles de confianza dentro del sistema emSign PKI definido incluyen varios roles como Oficial de administración, Oficial de auditoría, Oficial de registro, Oficial de seguridad, Oficial de sistemas, etc. Estos se definen en detalle junto con sus responsabilidades como parte de los documentos de política interna, y pueden ser confidenciales. en naturaleza.

### 28.2.2. NÚMERO DE PERSONAS REQUERIDAS POR TAREA

emSign asigna al menos dos personas a cada rol de confianza para evitar la posibilidad de un compromiso accidental o intencional de cualquier componente de la infraestructura de la EC de SoftNet. Ésta requiere que al menos dos personas que actúen en un rol confiable tomen medidas que requieran un rol confiable, como activar las claves privadas de la EC emisora, generar un par de claves EC o crear una copia de seguridad de una clave privada EC. Dichas operaciones sensibles también requieren la participación activa y la supervisión de la alta dirección.
La EC de SoftNet, como EC emisora de emSign PKI, utiliza prácticas comercialmente razonables para garantizar que una persona que actúe sola no pueda eludir las salvaguardas. Utiliza esfuerzos comercialmente razonables para identificar a un individuo separado para cada rol de confianza. Asegura que ningún individuo pueda obtener acceso a ninguna clave privada (que no sea la propia clave privada del individuo).

### 28.2.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

La EC de SoftNet, como EC emisora de emSign PKI, realiza un procedimiento de detección de seguridad adecuado, incluida la verificación de antecedentes antes de designar a una persona para el puesto de confianza. Cada función descrita aquí se identifica y autentica de manera que se garantice que la persona adecuada tenga la función adecuada para apoyar a la EC.

### 28.2.4. ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES

La EC de SoftNet hace cumplir la separación de roles para cada una de las funciones y el personal de confianza individual será designado específicamente para las funciones identificadas y definidas en la CP / CPS de emSign PKI y/o como parte de los procedimientos operativos de la EC de SoftNet.
No está permitido que ninguna persona sirva en más de un rol al mismo tiempo, para una actividad o tarea específica.

## 28.3. GESTIÓN DEL PERSONAL

La EC de SoftNet, como EC emisora de emSign PKI, realiza verificaciones de antecedentes apropiadas de todas las personas seleccionadas para asumir un rol de confianza de acuerdo con el procedimiento de inspección de seguridad designado, antes del comienzo de sus funciones. SoftNet determina la naturaleza y el alcance de cualquier verificación de antecedentes, a su exclusivo criterio.
SoftNet no será responsable de la conducta de los empleados que esté fuera de sus funciones y sobre la cual la EC no tenga control, incluidos, entre otros, actos de espionaje, sabotaje, conducta criminal o interferencia maliciosa.
Todos los empleados, agentes o contratistas independientes que desempeñen funciones de confianza estarán sujetos a estos requisitos de controles de personal.

### 28.3.1. REQUISITOS SOBRE LA CUALIFICACIÓN, EXPERIENCIA Y CONOCIMIENTO PROFESIONALES

La EC de SoftNet, como EC emisora de emSign PKI, requiere que el personal cumpla con un cierto estándar mínimo con respecto a los antecedentes, calificaciones, experiencia y requisitos de autorización para cada rol confiable. La selección del personal se realiza según este criterio.

### 28.3.2. PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES

Los procedimientos de verificación de antecedentes incluyen, entre otros, verificaciones y confirmación de:

- Empleo anterior
- Referencias profesionales
- Preparación académica
- Verificación de identidad
- Otros registros gubernamentales relevantes (por ejemplo, identificadores nacionales, etc.)

Cuando no se puedan obtener las verificaciones y confirmaciones debido a una prohibición o limitación de la ley u otras circunstancias, toda EC emisora de emSign PKI utilizará técnicas de investigación sustitutivas disponibles que brinden información similar, incluidas las verificaciones de antecedentes realizadas por agencias gubernamentales y/o privadas aplicables.

### 28.3.3. REQUISITOS DE FORMACIÓN

El personal implicado en emSign PKI, incluyendo la EC de SoftNet, seguirán un plan de formación interna adaptada a sus atribuciones asignadas. Esta formación será compatible con las normas de la industria, como las directrices del CA/Browser Forum.

### 28.3.4. REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN DE FORMACIÓN

Se requieren sesiones de actualización para todo el personal involucrado en el caso del medio ambiente, la tecnología y/o cambios operativos. Los cambios en las prácticas y/o políticas se comunican a todo el personal involucrado.

### 28.3.5. FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS

No se estipula.

### 28.3.6. SANCIONES POR ACTUACIONES NO AUTORIZADAS

En caso SoftNet o emSign, como su proveedor de servicios certificación, detecte una acción no autorizada, emprenderá las acciones disciplinarias necesarias. Cualquier acción que (intencionalmente o no) contraviene la Declaración de Prácticas de Certificación.

Tras la detección de una acción no autorizada, emSIgn iniciará un proceso de investigación. Durante este proceso se evitará que las personas involucradas obtengan acceso a los sistemas e información de emSign.
Las medidas disciplinarias serán tomadas después de la investigación determine la gravedad y la intención de la acción.

#### 28.3.7. REQUISITOS DE CONTRATACIÓN DE TERCEROS

Se requiere que los contratistas externos estén de acuerdo con las Políticas de seguridad de la información de emSign, y el personal temporal no amparado por un acuerdo de confidencialidad existente también estará obligado a firmar el acuerdo de confidencialidad antes de concederse el acceso a los recursos de información.
El acuerdo se examina cuando existen cambios en las condiciones de empleo o contratos.

#### 28.3.8. DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

A todo el personal incorporado dentro de emSign se le proporciona el acceso a por lo menos la siguiente información:

- Declaración de Prácticas de Certificación
- Políticas de Certificación
- Política de Privacidad
- Política de Seguridad
- Organigrama y funciones y responsabilidades asignadas
- Procedimientos operacionales
- Procedimientos de respuesta a incidentes

#### 28.3.9. FIN DEL CONTRATO Y PROCEDIMIENTO DE CAMBIO DE ROLES ASIGNADOS

En el caso de que un contrato finalice o se cambie el papel asignado a una persona, emSign se asegura de que se ejecute el procedimiento correspondiente. Este procedimiento incluye al menos los cambios necesarios en los privilegios concedidos a las instalaciones de acceso, sistemas de información y documentación.
El material asignado (tarjetas inteligentes, ordenadores, etc.) será devuelto o reasignado como sea necesario.
El cambio o terminación será notificado a todas las partes involucradas.

## 28.4. PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

#### 28.4.1. TIPOS DE EVENTOS REGISTRADOS

El registro de auditoría se mantendrá para:

1. Eventos de EC y Administración del Ciclo de Vida del Certificado:
    a. Se registra la generación, certificación, respaldo, recuperación y / o destrucción de los pares de claves de CA. Esto incluye todos los datos de configuración utilizados en el proceso.
    b. Solicitudes de certificados exitosas y no exitosas, emisiones de certificados, reemisiones de certificados y renovaciones de certificados para certificados de suscriptor. Además, las solicitudes de revocación del Certificado de Suscriptor, incluido el motivo de revocación.
    c. Generaciones y emisiones de CRL.
    d. Custodia de llaves, dispositivos y medios que contienen llaves.

e. Compromiso de una clave privada.

2. Eventos relacionados con la seguridad:
   a. Actividades de firewall y enrutador.
   b. Cualquier tiempo de inactividad en el sistema, bloqueos de software y fallas de hardware.
   c. Acciones del sistema de CA realizadas por personal de confianza, incluidas actualizaciones de software, reemplazos de hardware y actualizaciones.
   d. Intentos exitosos y fallidos de acceso al sistema PKI.
   e. Eventos del módulo de seguridad de hardware criptográfico, como uso, desinstalación, servicio o reparación y retiro.
   f. Entrada / salida de instalaciones de CA.
   g. Cada movimiento de los medios extraíbles
3. Información de solicitud de certificado:
   a. Toda la documentación e información relacionada proporcionada por el solicitante para el proceso de validación de la solicitud.
   b. Ubicaciones físicas y / o de almacenamiento electrónico de los documentos proporcionados por el solicitante.

Todos los registros incluyen los siguientes elementos:

- Fecha y hora de entrada
- Número de secuencia de entrada
- Descripción de la entrada.
- Identidad de la persona / dispositivo que realiza la entrada del registro

Se generarán y mantendrán los archivos de registro de auditoría para todos los eventos relacionados con la seguridad y los servicios de la CA emisora. Siempre que sea posible, los registros de auditoría de seguridad se generarán automáticamente. Cuando esto no sea posible, se utilizará un libro de registro en papel u otro mecanismo físico. Los registros de auditoría de seguridad de todos los eventos mencionados anteriormente se conservarán y estarán disponibles durante las auditorías de cumplimiento.

El acceso a los sistemas está protegido por Crypto Tokens protegidos con PIN o en forma de nombre de usuario - contraseña, según lo requiera un sistema, software o base de datos específicos. Se garantiza que las contraseñas administrativas en tales casos se dividan, de modo que se requerirá un mínimo de dos personas para realizar una actividad crítica / administrativa.

### 28.4.2. FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA (LOG)

Los registros de auditoría se verificarán al menos una vez al mes para ver si hay evidencia de actividad maliciosa.

### 28.4.3. PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA

El período de retención para los registros de auditoría para todas las EC emisoras de emSign PKI será el siguiente:

1. Registros de la actividad de gestión de claves de EC 30 años
2. Registros del sistema de EC de la actividad de gestión de certificados 30 años
3. Sistema operativo registra 7 años
4. Sistema de acceso físico registra 7 años
5. Registros manuales de acceso físico 7 años
6. Grabación de video del acceso a las instalaciones de EC 90 días

#### 28.4.4. PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

En todas las EC emisoras de emSign PKI, los registros de auditoría están protegidos mediante una combinación de controles de acceso físicos y lógicos. Los eventos se registran de manera que no se puedan eliminar ni destruir por ningún período de tiempo que se retengan. Los eventos se registran de manera que se garantice que solo las personas con acceso de confianza autorizado puedan realizar cualquier operación en función de su perfil sin modificar la integridad, la autenticidad y la confidencialidad de los datos.
Los registros de eventos están protegidos de una manera para evitar alteraciones y detectar alteraciones.

#### 28.4.5. PROCEDIMIENTOS DE BACKUP DE LOS REGISTROS DE AUDITORÍA

Todas las EC emisoras de emSign PKI deben realizar diariamente una copia de seguridad in situ de los registros de auditoría generados por el sistema. Al menos una vez al mes, todos los registros de auditoría y resúmenes de auditoría se realizarán en una ubicación segura fuera del sitio. Estos estarán bajo el control de un rol de confianza autorizado. La copia de seguridad del registro de auditoría debe protegerse en el mismo grado que los originales.
Los registros de auditoría están respaldados mediante procedimientos graduales y remotos.

#### 28.4.6. SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

El proceso de auditoría de seguridad de cada EC emisora debe iniciarse al inicio del sistema y puede finalizar solo al apagar el sistema. El sistema de recopilación de auditorías debe garantizar la integridad y disponibilidad de los datos recopilados. Si es necesario, el sistema de recopilación de auditorías debe proteger la confidencialidad de los datos. En el caso de que ocurra un problema durante el proceso de la recopilación de auditoría, las EC emisoras deben determinar si suspender las operaciones de la EC emisora hasta que se solucione el problema.
Los datos de auditoría automatizados se generan y registran a nivel de aplicación, red y sistema operativo. El personal de confianza registra los datos de auditoría generados manualmente.

#### 28.4.7. NOTIFICACIÓN AL SUJETO CAUSA DEL EVENTO

Sin estipulación.

#### 28.4.8. ANÁLISIS DE VULNERABILIDADES

Todas las EC emisoras de emSign PKI realizarán evaluaciones de vulnerabilidad periódicas. Dichas evaluaciones de vulnerabilidad deberían centrarse en las amenazas internas y externas que podrían dar lugar a acceso no autorizado, manipulación, modificación, alteración o destrucción del proceso de emisión del Certificado.
Las evaluaciones de vulnerabilidad también incluirán el escaneo de la aplicación, así como las pruebas de penetración. Cualquier resultado negativo de dichos informes se someterá a acciones correctivas para dicho resultado negativo. No existirán vulnerabilidades de seguridad comunes en sitios web públicos, alojados en la red.
Los resultados de tales pruebas de evaluación de vulnerabilidad se utilizarán para mejorar la seguridad del medio ambiente.

## 28.5. ARCHIVO DE REGISTROS

Todas las EC emisoras de emSign PKI deberán mantener un archivo de los registros relevantes según las políticas de retención de registros establecidas en la CP / CPS de emSign y cualquier política de retención

de registros que aplique la ley. La EC incluirá detalles suficientes en los registros archivados para mostrar que se emitió un Certificado de conformidad con dicho CP / CPS.

#### 28.5.1. TIPOS DE EVENTOS ARCHIVADOS

Todas las EC emisoras de emSign PKI archivan registros que incluirán toda la evidencia relevante en posesión de la EC emisora, incluyendo:

- Registros de auditoría;
- Solicitudes de certificados digitales y todas las acciones relacionadas;
- Contenido de los certificados digitales emitidos;
- Evidencia de aceptación del Certificado Digital y Acuerdos de Titular del Certificado firmados (electrónicamente o de otro modo);
- Solicitudes de revocación y todas las acciones relacionadas;
- Solicitudes de archivo y recuperación;
- Listas de revocación de certificados digitales publicadas;
- Opiniones de auditoría como se discute en el emSign PKI CP / CPS; y

Para cada Certificado digital, los registros contienen información relacionada con la creación, emisión, uso previsto, revocación y caducidad. Previa solicitud autorizada, la EC pone a disposición documentación relacionada con cada Certificado digital sujeta a la Política de acceso a documentos PKI emSign.

#### 28.5.2. PERIODO DE CONSERVACIÓN

Todas las EC emisoras de emSign PKI archivan y retienen los registros de auditoría de acuerdo con la política de retención de registros de auditoría descrita en la CP / CPS de emSign.

#### 28.5.3. PROTECCIÓN DE ARCHIVOS

Todas las EC emisoras de emSign PKI archivan y protegen los registros de auditoría de acuerdo con la política de protección de registros de auditoría descrita en la CP / CPS de emSign.

#### 28.5.4. PROCEDIMIENTOS DE BACKUP DEL ARCHIVO DE REGISTROS

Todas las EC emisoras de emSign PKI mantienen e implementan procedimientos de copia de seguridad para que las copias de seguridad de los registros archivados se almacenen en una ubicación separada, de modo que en caso de pérdida o destrucción de los archivos primarios esté disponible un conjunto completo de copias de seguridad.

#### 28.5.5. REQUISITOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS

Todas las CA emisoras de emSign PKI marcarán automáticamente sus registros a medida que se creen. Todos los eventos que se registran en la PKI de emSign incluyen la fecha y la hora en que tuvo lugar el evento. Esta fecha y hora se basan en la hora del sistema en la que opera el sistema de CA. emSign PKI utiliza procedimientos para revisar y garantizar que todos los sistemas que operan dentro de emSign PKI se basan en una fuente de tiempo confiable.

#### 28.5.6. SISTEMA DE ARCHIVO DE LA INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

El sistema de recopilación de archivos de emSign PKI es interno.

#### 28.5.7. PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA

Solo los roles y auditores de confianza específicos pueden ver los archivos en su totalidad. La EC emisora puede permitir a los suscriptores obtener una copia de su información archivada. El contenido de los archivos no se divulgará, excepto según lo exija la ley.

## 28.6. CAMBIO DE CLAVES DE UNA EC

Para permitir una transición sin problemas de los certificados de EC vencidos, la nueva clave privada de EC se certificará hacia el final de la fecha de vencimiento del certificado anterior. La nueva clave privada y el certificado de EC se pondrán en servicio y se utilizarán para emitir nuevos certificados de suscriptor de aquí en adelante.
En este caso, las claves privadas de EC antiguas y nuevas pueden estar simultáneamente activas.
Las antiguas claves privadas de EC utilizadas para firmar los certificados de suscriptor anteriores se mantienen hasta el momento en que todos los certificados de suscriptor que se encuentran debajo expiren. Hasta entonces, la antigua clave privada se utilizará para fines que incluyen CRL y OCSP.

## 28.7. RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE Y DESASTRE NATURAL U OTRO TIPO DE CATÁSTROFE

El Plan de Recuperación y Desastre de Operaciones de EC está en vigencia con todas las EC bajo emSign PKI, en forma de Plan de Continuidad de Negocio. Este plan cumple el propósito de restaurar las operaciones comerciales centrales cuando las operaciones y / o sistemas se han visto afectados de manera adversa y significativa. Esta restauración se realizará lo más rápido posible. Dicho plan proporcionará la reanudación inmediata de los servicios de revocación en caso de una emergencia inesperada.
El plan de recuperación ante desastres y reanudación comercial es propietario, sensible a la seguridad y confidencial. Por consiguiente, no se pretende que esté disponible de manera general.
Todas las EC emisoras bajo emSign PKI han implementado un plan de compromiso de clave apropiado que detalla las actividades tomadas en caso de compromiso de una clave privada de EC emisora emSign. Dichos planes incluyen procedimientos para:

- Revocación de todos los certificados digitales firmados con la clave privada de esa emSign emisora de EC;
- Notificar a la EC de SoftNet y a todos los titulares de certificados digitales emitidos por dicha EC.

#### 28.7.1. PLAN DE CONTINUIDAD DEL NEGOCIO

El Plan de Continuidad del Negocio es estrictamente confidencial y prevé:

- Procedimientos de compromiso de clave privada, así como procedimientos de revocación de clave pública.
- Procedimientos de manejo de incidentes y compromisos.
- Software, recursos informáticos y / o procedimientos de manejo de datos corruptos.
- Capacidades y procedimientos de continuidad del negocio después de un desastre.

El plan de continuidad del negocio y los planes de seguridad se ponen a disposición de los auditores y se auditan durante los ciclos de auditoría definidos. Estos también están sujetos a pruebas anuales, revisión y actualización de los procedimientos.

## 28.8. CESE DE UNA EC O ER

Cuando sea necesario terminar un servicio de EC emisora o de Entidad de Registro, emSign PKI deberá

- Proporcionar notificación e información sobre la terminación enviando una notificación por correo electrónico a sus clientes, proveedores, certificadores cruzados (si corresponde) y cualquier otra entidad aplicable.
- Al publicar dicha información en el sitio web
- Minimice cualquier interrupción causada por la terminación de una EC emisora
- Cuidar la retención de los registros archivados de la EC emisora
- Verificar y transferir todas las responsabilidades a una entidad sucesora calificada.

Todas las EC bajo emSign PKI especifican los procedimientos que seguirán al finalizar la totalidad o una parte de sus operaciones de emisión y gestión de certificados digitales.

La EC sucesora debe asumir las mismas obligaciones, deberes y derechos de la terminación de la EC, y emitir nuevas claves / certificados a todos los usuarios cuyas claves / certificados fueron revocados por la terminación de la EC. Dicha nueva emisión de certificado deberá cumplir, el usuario que realiza una solicitud y cumple con los requisitos de identificación y autenticación, así como con el acuerdo del suscriptor de la nueva EC emisora.

Cuando sea práctico, la revocación de Certificados Digitales / Claves se cronometrará para que coincida con el despliegue progresivo y planificado de nuevas Claves y Certificados Digitales por parte de un sucesora EC emisora.

# 29. CONTROLES TÉCNICOS DE SEGURIDAD

La Autoridad de Certificación de emSign ha implementado suficientes controles de seguridad para proteger las claves privadas y el acceso a varios módulos dentro del entorno de la Entidad de Certificación.

Las claves privadas de EC emisoras se almacenan de forma segura en un módulo de seguridad de hardware que cumple con el estándar FIPS 140-2 Nivel 3+. El acceso a los sistemas / módulos dentro del entorno de la Entidad de Certificación está restringido usando tokens o tarjetas inteligentes y frases de paso asociadas de tal manera que ningún miembro individual tenga el control total sobre ningún componente del sistema. Los módulos de seguridad de hardware siempre se almacenan en un entorno físicamente seguro que está sujeto a control de seguridad.

## 29.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

### 29.1.1. GENERACIÓN DEL PAR DE CLAVES

La emisión de pares de claves de EC se genera de manera segura como parte de una ceremonia clave en un entorno de confianza física por parte de personal de confianza. La emisión de la generación de claves de EC se lleva a cabo en un dispositivo seguro que cumple al menos con FIPS 140-2 Nivel 3.

Pares de claves de suscriptor:

1. Son generados por el suscriptor de manera segura, ya sea en hardware o software, antes de enviar una solicitud de certificado digital.
2. Diferir en sus métodos de generación de claves de acuerdo con la clase o tipo de certificado digital solicitado.
3. Para ciertos tipos de certificados como la firma de Adobe, etc., se generarán en un medio que cumpla con los estándares de certificación FIPS 140-1 Nivel 2+ y también evite la exportación o duplicación de claves.

emSign PKI se reserva el derecho de generar pares de claves de suscriptor, según el tipo o clase del certificado, en el escenario que necesita emSign PKI para generar dichos pares de claves.

### 29.1.2. ENTREGA DE LA CLAVE PRIVADA A LOS TITULARES

Según corresponda en la mayoría de los casos, si el Suscriptor o el titular de la clave prevista genera la clave privada, entonces no hay necesidad de entregar la Clave privada. Si alguien que no sea el titular de la clave previsto está generando la clave en nombre del titular de la clave prevista, debe garantizar que se mantenga una seguridad suficiente dentro del proceso de generación de claves y cualquier proceso de emisión posterior al Suscriptor. En todo momento, el acceso a la clave privada debe estar protegido por un PIN proporcionado por el suscriptor.

### 29.1.3. ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

Las claves públicas deben entregarse a la EC emisora de manera segura y confiable de manera que vincule la identidad verificada del suscriptor con la clave pública. El proceso de solicitud debe garantizar que la clave pública no se haya modificado durante el tránsito y que el remitente posea la clave privada correspondiente a la clave pública transferida.

### 29.1.4. ENTREGA DE LA CLAVE PÚBLICA DE LA EC A TERCEROS ACEPTANTES

Todas las EC emisoras de emSign PKI se asegurarán de que la entrega de la clave pública a las partes confiables se realice de manera segura para servir como un ancla de confianza en los navegadores comerciales y almacenes raíz del sistema operativo, o puede especificarse en un archivo de política de validación de certificado o descubrimiento de ruta. La EC puede entregar su certificado de clave pública a través de su repositorio disponible en el sitio web de emSign o del emisor.

### 29.1.5. TAMAÑO DE LAS CLAVES

Las longitudes de clave y los algoritmos clave dentro de la PKI de emSign están determinados por los perfiles de certificado.
Para los certificados de suscriptor, emSign PKI garantiza el uso de una longitud mínima de clave de certificados de módulo de 2.048 bits para algoritmos RSA / DSA y una longitud mínima de clave de 256 bits para algoritmos ECC. En todo momento, la emisión de EC garantizará que las longitudes de las claves se alineen con los requisitos de referencia y las pautas de EV.
Se deben tener en cuenta los siguientes puntos en los algoritmos Hash:

1. Todos los algoritmos de firma se utilizan junto con el algoritmo implícito de SHA-256 o un algoritmo hash que es igual o más resistente a un ataque de colisión.
2. MD5 no es compatible.

### 29.1.6. PARÁMETROS DE GENERACIÓN DE LA CLAVE PÚBLICA Y VERIFICACIÓN DE LA CALIDAD

Todas las claves de EC se generan en hardware calificado FIPS 140-2 y cumple con los Todas las claves de CA se generan en hardware calificado FIPS 140-2 y cumple con los requisitos de FIPS 1862, lo que garantiza los parámetros adecuados y su calidad para las claves públicas.
Se utilizan técnicas razonables para validar la idoneidad de las claves públicas del suscriptor. Cualquier clave débil conocida se probará y rechazará en el momento de la presentación.

### 29.1.7. USOS PERMITIDOS DE LA CLAVE (SEGÚN EL CAMPO KEY USAGE DE LA X.509)

El "uso de clave" de emSign PKI Root EC permite que firme sus EC subordinadas, las CRL y otros fines necesarios definidos en la sección Perfiles de certificado de la CP / CPS de emSign PKI. Del mismo modo, el "uso de clave" de las EC emisoras bajo emSign PKI (lo que incluye a la EC de SoftNet) permite la firma de certificados de suscriptor y otros propósitos definidos en la sección Perfiles de certificado de la CP / CPS de emSign PKI.

Las claves de suscriptor se utilizarán para la firma digital, el cifrado de claves, el cifrado de datos y otros fines definidos en la sección Perfiles de certificado de la CP / CPS de emSign PKI y en este documento.

## 29.2. PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

La emisión de certificados de EC, RA, suscriptores y otros participantes deben tomar las medidas adecuadas y adecuadas para proteger las claves privadas de acuerdo con los requisitos indicados en la CP / CPS de emSign PKI.
Esto incluye:

- Asegurar su clave privada
- Tomar las precauciones necesarias para evitar la pérdida, daño, divulgación, alteración o acceso o uso no autorizado de su clave privada
- Ejercer el control y uso exclusivo y completo de la clave privada

### 29.2.1. CONTROLES Y ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS

Todas las claves privadas de la EC de SoftNet, bajo emSign PKI, deben generarse y mantenerse en un módulo de seguridad de hardware que cumpla con los estándares federales de protección de la información 140-2 nivel 3+.
Los requisitos para los dispositivos criptográficos de usuario final (si los hay) pueden variar en términos del nivel de seguridad esperado.

### 29.2.2. CONTROL MULTIPERSONA (N DE M) DE LA CLAVE PRIVADA

Todas las claves privadas de CA del emisor se acceden / activan en CA System a través del control de varias personas de confianza n-de-m, incluidas las copias de seguridad de claves privadas.

### 29.2.3. CUSTODIA DE LA CLAVE PRIVADA

Las claves privadas de CA no están en custodia.
Las Claves de firma del suscriptor no estarán en custodia. Sin embargo, las CA emisoras bajo emSign PKI pueden custodiar las claves de cifrado del suscriptor, a fin de proporcionar la recuperación de claves.

### 29.2.4. BACKUP DE LA CLAVE PRIVADA

Las CA emisoras bajo emSign PKI pueden hacer una copia de seguridad de sus claves privadas utilizando un dispositivo criptográfico seguro y almacenar las claves privadas en un estado cifrado si las claves privadas se almacenan fuera del módulo criptográfico.
Los suscriptores pueden optar por hacer una copia de seguridad de sus claves privadas de manera segura. La CA emisora puede proporcionar servicios de copia de seguridad de la clave privada para el suscriptor, siempre que las copias de seguridad se aseguren de manera que solo el suscriptor pueda controlar la clave privada.

### 29.2.5. ARCHIVO DE LA CLAVE PRIVADA

Después de la expiración de los Certificados de CA, el par de claves asociado se conservará de forma segura durante un período mínimo de 5 años. Tal almacenamiento de archivo debe cumplir con el requisito de almacenamiento de clave privada (en módulo criptográfico). Dichas claves archivadas no se utilizarán para ninguna firma de producción.

Las CA emisoras bajo emSign PKI pueden archivar copias de las claves privadas del suscriptor. Las claves privadas que se archiven deben mantenerse al menos en el mismo nivel de seguridad que cuando se creó originalmente el par de claves. Las claves de firma no se archivarán. Las claves privadas no se archivan para cualquier participante PKI.

### 29.2.6. TRANSFERENCIA DE LA CLAVE PRIVADA A/DESDE EL MÓDULO CRIPTOGRÁFICO

Las claves de CA siempre se generan en módulos criptográficos. Se copian en módulos criptográficos similares para fines de recuperación / continuidad del negocio. Dicha copia también se realizará en forma cifrada, y la clave privada nunca debe existir en forma de texto sin formato fuera del módulo criptográfico.
El proceso de descarga de las claves privadas se realiza según procedimiento del dispositivo criptográfico y se almacenan de forma segura protegidas por claves criptográficas con control dual.

### 29.2.7. ALMACENAMIENTO DE LAS CLAVES PRIVADAS EN UN MÓDULO CRIPTOGRÁFICO

Las claves privadas de CA se almacenarán en un módulo de seguridad de hardware que cumpla con el estándar FIPS 140-2 Nivel 3.
Las claves privadas del suscriptor se pueden almacenar en un módulo criptográfico.

### 29.2.8. MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

Las claves privadas de CA se activan de acuerdo con las especificaciones del fabricante del módulo criptográfico.
Las claves privadas del suscriptor deben estar protegidas / activadas con un PIN o contraseña.

### 29.2.9. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

Cuando no esté en uso, la CA emisora desactivará sus claves privadas al finalizar (cerrar sesión) las sesiones con módulos criptográficos. Estos se basan en las especificaciones del fabricante del módulo criptográfico.
Por otro lado, la desactivación de las claves privadas de las ER o de los usuarios finales basados en hardware, se realiza mediante la extracción del dispositivo de seguridad (tarjeta inteligente u otros cripto-tokens aceptados) de la estación de trabajo donde es utilizada.
La desactivación de otras claves privadas del usuario final, mientras que no se encuentran basadas en el hardware, se lleva a cabo mediante el apagado del dispositivo en el que se almacena la clave privada.
El suscriptor debe tomar todas las medidas razonables para evitar el uso no autorizado del dispositivo.

### 29.2.10. MÉTODO PARA DESTRUIR LA CLAVE PRIVADA

La entidad emisora de certificados utilizará a individuos en roles de confianza para destruir las claves privadas cuando ya no sean necesarias o al vencimiento o al revocar el certificado eliminando o sobrescribiendo los datos o utilizando la destrucción física.
Los suscriptores pueden destruir sus claves privadas cuando se revoca o vence el certificado correspondiente si la clave privada ya no es necesaria. Esto debe hacerse de manera segura para garantizar que no haya pérdida, robo, compromiso o divulgación o uso no autorizado.

### 29.2.11. EVALUACIÓN DEL MÓDULO CRIPTOGRÁFICO

La calificación del Módulo criptográfico deberá cumplir con los requisitos establecidos en la sección "Estándares y controles del módulo criptográfico" de este documento.

## 29.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

### 29.3.1. ARCHIVO DE LA CLAVE PÚBLICA

El emisor CA archivará una copia de cada clave pública.

### 29.3.2. PERIODOS OPERATIVOS DE LOS CERTIFICADOS Y PERIODO DE USO DEL PAR DE CLAVES

Los períodos de validez máximos para los Certificados digitales emitidos dentro de la PKI de emSign CA son:

| Tipo | Uso de la clave privada (firmado de certificados | Uso de la clave privada (firmando CRL) | Duración del certificado |
|---|---|---|---|
| Certificado Raíz EC | 20 años | 25 años | 25 años |
| Todas las ECs Subordinadas de la Raíz EC | 12 años | 15 años | 15 años |
| Certificados de suscriptor con Server Authentication EKU | No aplica | No aplica | 825 días |
| Otros certificados de suscriptor | No aplica | No aplica | 39 meses (o el máximo permitido según las guías correspondientes) |
| Todos los demás certificados digitales | No aplica | No aplica | Sin estipulación (o el máximo permitido según las guías correspondientes) |

Para todos los certificados, incluidos los certificados de suscriptor o cualquier CA subordinada, la fecha de finalización del certificado no excederá la fecha de finalización de su certificado de firma (emisor).

## 29.4. DATOS DE ACTIVACIÓN

### 29.4.1. GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

La CA emisora generará datos de activación que tengan la fuerza suficiente para proteger sus claves privadas de abonado, incluidos métodos como la autenticación de dos factores.
Los oficiales de PKI de emSign también deben usar contraseñas seguras para evitar aún más el acceso no autorizado a los sistemas de CA.

#### 29.4.2. PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Si los datos de activación deben transmitirse a los suscriptores, se realizarán a través de un canal de protección adecuada y distinto en tiempo y lugar del Módulo criptográfico asociado. Los códigos de identificación personal se pueden suministrar al suscriptor de manera segura.

#### 29.4.3. OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Cuando se utiliza un PIN o frase de contraseña, el usuario debe ingresar el PIN o frase de contraseña junto con otros detalles de identificación personal para poder acceder e instalar sus claves o certificados digitales.

## 29.5. CONTROLES DE SEGURIDAD INFORMÁTICA

emSign PKI, como proveedor de servicios de certificación de SoftNet, tiene una Política de seguridad de la información que documenta las políticas, estándares y pautas relacionadas con la seguridad de la información. Esta Política de Seguridad de la Información ha sido aprobada por la Autoridad de Políticas de emSign y se comunica a todos los empleados que pertenecen a emSign PKI.
Algunos de los controles y políticas de seguridad incluyen:

- Procesos, sistemas y salvaguardas claramente definidos para garantizar el acceso físico y lógico a los sistemas.
- Uso de HSM para la protección de la emisión de material de clave privada de EC.
- Controles de acceso a los servicios de la Autoridad de certificación y roles PKI.
- Separación forzada de funciones para los Servicios de Autoridad de Certificación y los roles de PKI.
- Verificaciones de personal de confianza, roles de responsabilidad en la PKI de emSign.
- Seguridad de aplicaciones, sesiones y bases de datos.
- Proceso de archivo para el historial de la autoridad de certificación y los datos de auditoría.
- Existen controles para evitar que se ejecute software no autorizado o ilegítimo dentro de sus sistemas, incluidos, entre otros, software antivirus y antimalware.
- Plan integral de respuesta a incidentes para responder al compromiso o incumplimiento de sus sistemas en línea, así como sus sistemas de emisión de certificados.
- Aplicación de la autenticación multifactor para todas las cuentas capaces de causar directamente la emisión de un certificado.

#### 29.5.1. EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

Sin estipulación.

## 29.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA

Se deben seguir los siguientes controles del ciclo de vida para garantizar la mitigación del riesgo durante la operación del ecosistema emSign PKI.

- El hardware y el software adquiridos deben seguir metodologías que garanticen que no se pueda manipular ningún componente en particular.
- Los sistemas utilizados dentro de emSign PKI se desarrollarán utilizando estrictos procedimientos de control de cambios
- Solo el personal de confianza estará autorizado para usar los sistemas centrales de emSign PKI
- La EC emisora no instalará aplicaciones o software de componentes que no forme parte de la configuración de la EC emisora

- La EC emisora deberá comprar o desarrollar actualizaciones de la misma manera que el equipo original, y utilizará personal capacitado de confianza para instalar el software y el equipo.
- Los administradores de sistemas en la red no tienen acceso a los sistemas de emisión de certificados debido a la segmentación adecuada de los deberes y los principios de privilegios mínimos.

#### 29.6.1. CONTROLES DE DESARROLLO DE SISTEMAS

Se implementan controles adecuados para el desarrollo de sistemas de la siguiente manera

- Se siguen las prácticas del ciclo de vida del desarrollo de software para el desarrollo e implementación de nuevos sistemas.
- El análisis de seguridad se realiza en la etapa de diseño.
- La subcontratación de proyectos (si existe) se supervisa y controla de cerca.

#### 29.6.2. CONTROLES DE GESTIÓN DE SEGURIDAD

La emisión de la instalación de EC, la configuración, así como cualquier modificación, se documentan y controlan mediante la emisión de EC a través de mecanismos formales.

El proceso de control de cambio de la EC emisora incluirá procedimientos para detectar modificaciones no autorizadas a los sistemas EC emisores. Cualquier software de terceros adquirido se verificará para su integridad, versiones apropiadas y para estar libre de modificaciones.

#### 29.6.3. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

emSign PKI verifica periódicamente la integridad del software de la Entidad de Certificación y monitorea la configuración de los sistemas EC.

## 29.7. CONTROLES DE SEGURIDAD DE LA RED

emSign PKI, como proveedor de servicios de certificación de SoftNet, se asegura de que la red en la que está alojado el sistema EC esté protegida por firewalls de red y otros sistemas que, en la medida de lo posible, eviten el acceso no autorizado de las partes. Otras medidas incluyen

- Desactivar los puertos o servicios de red no utilizados.
- Los cortafuegos y enrutadores de filtrado utilizados para los equipos de CA limitan los servicios hacia y desde el equipo de EC a los necesarios para realizar las funciones de EC.
- Mantener controles de seguridad de red que cumplan como mínimo los requisitos de seguridad del sistema de redes y certificados.
- Verifique la emisión incorrecta de certificados, especialmente para dominios de alto perfil.
- Cierre la emisión de certificados rápidamente si se nos alerta de intrusión.
- Revise la infraestructura de red, el monitoreo, las contraseñas, etc. en busca de signos de intrusión o debilidad.
- Asegúrese de que los sistemas IDS (Sistema de detección de intrusiones) e IPS (Sistema de prevención de intrusiones) y otro software de monitoreo estén implementados y actualizados.
- Segmentación de sistemas clave de emisión de certificados de servidores y sistemas no relacionados, como sitios web de marketing, etc.

## 29.8. SELLADO DE TIEMPO

Las EC emisoras se asegurarán de que sus componentes se sincronicen regularmente con un servicio horario, como un reloj atómico o un protocolo de tiempo de red. La hora del sistema en las computadoras

se actualizará utilizando el Protocolo de hora de red (NTP) para sincronizar los relojes del sistema al menos una vez cada ocho horas.
Esto se utilizará para establecer el tiempo de

- Tiempo de validez inicial de un certificado de CA;
- Revocación de un certificado de CA;
- Publicación de actualizaciones de CRL; y
- Emisión de certificados de suscriptor

Se mantiene un servidor NTP interno que se sincroniza con fuentes externas y mantiene la precisión de su reloj en un segundo o menos.
Además, se opera una Autoridad de sello de tiempo (TSA) de emSign para ofrecer servicios de sellado de tiempo de acuerdo con RFC 3161, así como para los sellos de tiempo de Microsoft Authenticode.

# 30. PERFILES DE CERTIFICADOS, CRL Y OCSP

## 30.1. PERFIL DE CERTIFICADO

Todos los certificados digitales de la EC de SoftNet cumplen con los perfiles de Certificado digital y Lista de revocación de certificados como se describe en RFC 5280 y utilizan los estándares de Certificado digital ITU-T X.509 versión 3.
Consulte el APÉNDICE B para ver los contenidos del Certificado que son específicos de las clases individuales de Certificados Digitales.

### 30.1.1. NÚMERO DE VERSIÓN

Todos los certificados son certificados X.509 versión 3.

### 30.1.2. KEY USAGE

Esto permite fijar los valores de uso de clave estándar. El campo de criticidad de la extensión KeyUsage generalmente se establece en TRUE.

### 30.1.3. EXTENSIONES DEL CERTIFICADO

Los certificados tienen las extensiones requeridas por los respectivos perfiles de certificado. Las extensiones privadas son permisibles, pero el uso de extensiones privadas no está garantizado bajo este documento a menos que se incluya específicamente como referencia.

### 30.1.4. EXTENSIÓN DE POLÍTICAS DE CERTIFICADO

Un identificador de objeto (OID) es un número único que identifica un objeto o política, sin ambigüedades. La extensión CertificatePolicies se completa con el OID para los identificadores de política definidos en la CP / CPS de emSign. El campo de criticidad de esta extensión se establecerá en FALSO.
Esto puede contener identificadores de política adicionales según lo requerido por las pautas de CABF, los requisitos del Certificado de Adobe, etc

#### 30.1.4.1. IDENTIFICADORES DE POLÍTICA DE CERTIFICADOS RESERVADOS

Las EC emisoras de emSign utilizarán opcionalmente los identificadores de política relacionados con DV, OV y IV de los requisitos de referencia del CA Browser Forum para afirmar el cumplimiento respectivo. El campo subject también deberá contener los valores de conformidad con los requisitos DV, OV y IV, según corresponda.

#### 30.1.4.2. CERTIFICADOS DE EC RAÍZ

Los certificados de CA raíz de emSign no deben contener esta extensión.

#### 30.1.4.3. CERTIFICADOS EC SUBORDINADA

Las propias EC subordinadas de emSign PKI contienen el identificador "anyPolicy" (2.5.29.32.0) o un identificador de política explícito para confirmar el cumplimiento de la política.
Sin embargo, las EC subordinadas externas deberán contener solo identificadores de política explícitos para confirmar el cumplimiento de la política. No contendrá el identificador "anyPolicy" (2.5.29.32.0).

#### 30.1.4.4. CERTIFICADOS DE SUSCRIPTOR

Los certificados de suscriptor emitidos por las EC subordinadas deberán contener una o más ID de política.

- Una de esas ID de política puede indicar la ID de política de CPS y la URL, para confirmar la adhesión y el cumplimiento de la CP / CPS de emSIgn.
- También deberá contener una identificación de la política que indique el cumplimiento de la verificación, la emisión y el cumplimiento del certificado del certificado respectivo, según los Apéndices A y B. Dicha identificación de la política se referirá a la Sección 1.2 de este documento.

### 30.1.5. IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS

El certificado contiene la información del Algoritmo de firma según las especificaciones del RFC 5280.

### 30.1.6. FORMATOS DE NOMBRES

Los certificados con formato de nombre cumplen con RFC 5280. Cada certificado incluye un número de serie de certificado único (no secuencial) entre las respectivas EC emisoras, que exhibe al menos 20 bits de entropía.
El Nombre del Emisor se completará en cada Certificado emitido que contenga el País, el Nombre de la Organización y el Nombre Común del Emisor CA. El nombre distinguido para cada tipo de certificado se establece según el perfil de certificado respectivo. Los subcampos opcionales en el Asunto solo contienen información verificada o se dejan vacíos. Los campos de asunto no deben contener valores como metadatos de punto, guión, espacio vacío, etc. (por ejemplo: '.' o '-' OR ' ') indicando que el campo no es aplicable.
Después del 30 de abril de 2019, la extensión del nombre alternativo del sujeto (subjectAltName) no deberá contener caracteres de subrayado ("_") en las entradas de dNSName.

### 30.1.7. OTROS CAMPOS PRIMARIOS O EXTENSIONES

Sin estipulación, a menos que se defina específicamente para cada perfil de certificado.

## 30.2. PERFIL DE CRL

Las listas de revocación de certificados se emiten en el formato X.509 versión 2 de acuerdo con RFC 5280.

### 30.2.1. NÚMERO (S) DE VERSIÓN

La emisión de CA dentro del emSign PKI emite X.509 versión 2 Listas de revocación de certificados.

#### 30.2.2. CAMPOS EN CRL

La CRL contiene los siguientes campos:

1. DN del emisor
2. Fecha de vigencia de la emisión de CRL
3. Próxima fecha de actualización
4. Algoritmo de firma
5. Algoritmo de hash de firma

#### 30.2.3. EXTENSIONES DE CRL

CRL contiene las siguientes extensiones:

1. Número de CRL: número secuencial para CRL bajo un emisor específico.
2. Identificador de clave de autoridad: Identificador de la CA emisora.

#### 30.2.4. ENTRADAS DE CRL

CRL contiene las entradas de certificados revocados bajo ese emisor. Cada una de estas entradas contiene:

1. Número de serie del certificado
2. Fecha de revocación
3. Motivo de revocación

### 30.3. PERFIL OCSP

El emisor EC puede operar un respondedor de protocolo de estado de certificado en línea de conformidad con los requisitos necesarios. Los respondedores OCSP cumplen con RFC 5019.

#### 30.3.1. NÚMERO (S) DE VERSIÓN

La emisión de CA dentro del emSign PKI emite respuestas de OCSP de la Versión 1.

#### 30.3.2. CAMPOS EN RESPUESTAS OCSP

Las solicitudes y respuestas de OCSP deberán cumplir con los requisitos de RFC.

#### 30.3.3. EXTENSIONES OCSP

Sin estipulación

## 31. AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES

### 31.1. FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES

Las prácticas en este CP / CPS están diseñadas para cumplir o exceder los requisitos de los estándares de la industria generalmente aceptados y todas las EC emisoras de emSign PKI son auditadas anualmente para cumplir con la última versión de AICPA / CICA WebTrust para autoridades de certificación y el Programa de validación extendida.

### 31.2. IDENTIDAD/CUALIFICACIÓN DEL AUDITOR

Los servicios de auditoría externa son realizados por un "Auditor calificado" que es independiente, creíble, reconocido por AICPA / Webtrust con experiencia significativa en la realización de auditorías de seguridad de la información y tecnologías PKI y criptográficas. El "Auditor calificado" está obligado por la ley, la

regulación gubernamental o el código de ética profesional y mantiene un seguro de responsabilidad profesional / errores y omisiones con límites de póliza de al menos USD 1,000,000 en cobertura
Las auditorías de emSign PKI han sido realizadas por BDO.
El evaluador para SoftNet se seleccionará cuando se requiera una auditoría o evaluación. A cualquier empresa o profesional cuyos servicios son contratados como auditor o asesor, debe de cumplir los siguientes requisitos:

- Capacidad y experiencia suficiente y acreditada para realizar los servicios requeridos (PKI de auditoría, evaluación de seguridad, etc.). En particular, para las auditorías externas, se requiere acreditación adecuada para llevar a cabo auditorías WebTrust.
- En el caso de las auditorías externas, debe ser independiente de SoftNet a un nivel de organización.

## 31.3. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

emSign PKI ha seleccionado un auditor que es completamente independiente de emSign EC.
Para lo que le compete, la política de auditoría de SoftNet no permite ningún tipo de relación jurídica, organizativa o de otro tipo con el auditor externo que daría lugar a un conflicto de intereses.

## 31.4. ASPECTOS CUBIERTOS POR LOS CONTROLES

Los temas cubiertos por la evaluación incluyen, entre otros, la divulgación de prácticas de negocio de EC (CP / CPS), la integridad del servicio de emSign Operations y el cumplimiento operativo de emSign con su CP / CPS y las pautas de Webtrust.

## 31.5. ACCIONES A TOMAR COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS

Para cualquier incumplimiento material o deficiencia presentada por los Auditores, emSign y SoftNet, a su exclusivo criterio, determinarán un plan de acción correctiva apropiado con el marco de tiempo apropiado para eliminar la deficiencia.

## 31.6. COMUNICACIÓN DE RESULTADOS

Los resultados de la auditoría se informan a la Autoridad de Políticas para el análisis y la resolución de cualquier deficiencia a través de un plan de acción correctiva posterior.

## 31.7. AUTOAUDITORÍAS

emSign PKI y SoftNet controlan la calidad del servicio a través de auditorías internas continuas al menos trimestralmente, contra una muestra de certificados seleccionada al azar. El tamaño de la muestra de los certificados emitidos sería al menos del 3%. Este período de tamaño de muestra debe comenzar desde la primera vez que se emite el certificado, o inmediatamente después de que se tomó la muestra de autoauditoría anterior

# 32. OTROS ASUNTOS LEGALES Y COMERCIALES

## 32.1. TARIFAS

### 32.1.1. TARIFAS DE EMISIÓN O RENOVACIÓN DE CERTIFICADOS

SoftNet cobra una tarifa a sus clientes por la emisión y renovación de certificados. Las tarifas se indican a los clientes a través de una interfaz web adecuada o mediante materiales de ventas y marketing. Las tarifas se pueden cambiar de vez en cuando a discreción de SoftNet.

### 32.1.2. TARIFAS DE ACCESO A LOS CERTIFICADOS

SoftNet puede cobrar una tarifa de acceso por proporcionar acceso a sus bases de datos / repositorio de certificados.

### 32.1.3. TARIFAS DE REVOCACIÓN O ACCESO A LA INFORMACIÓN DE ESTADO

EmSign CA no cobrará ninguna tarifa por la revocación de un certificado. Además, no se le cobrará ninguna tarifa a una parte que confía para verificar la validez del certificado existente utilizando una CRL.
Sin embargo, SoftNet se reserva el derecho de cobrar una tarifa por proporcionar información del estado del certificado vía OCSP.

### 32.1.4. TARIFAS DE OTROS SERVICIOS

emSign PKI y SoftNet se reserva el derecho de cobrar una tarifa por el sello de tiempo y / o cualquier otro servicio adicional.

### 32.1.5. POLÍTICA DE REEMBOLSO

SoftNet proporcionará un reembolso a los suscriptores bajo ciertas circunstancias y sujeto a ciertas condiciones. Los detalles de estos estarán contenidos en el documento contractual correspondiente.

## 32.2. RESPONSABILIDAD

La EC dispondrá en todo momento de un seguro de responsabilidad civil en los términos que marque la legislación vigente en Perú.
La EC actuará en la cobertura de sus responsabilidades por sí o a través de la entidad aseguradora, satisfaciendo los requerimientos de los solicitantes de los certificados, de los Firmante/Titulares y de los terceros que confíen en los certificados.
Las responsabilidades de la EC incluyen las establecidas por la presente CPS, así como las que resulten de aplicación como consecuencia de la normativa peruana.
La EC será responsable del daño causado ante el Titular o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, respecto de:

- La exactitud de toda la información contenida en el certificado en la fecha de su emisión.
- La garantía de que, en el momento de la entrega del certificado, obra en poder del Titular, la clave privada correspondiente a la clave pública dada o identificada en el certificado. La garantía de que la clave pública y privada funcionan conjunta y complementariamente.
- La correspondencia entre el certificado solicitado y el certificado entregado.
- Cualquier responsabilidad que se establezca por la legislación vigente.

## 32.3. EXONERACIÓN DE RESPONSABILIDAD

La EC no será responsable en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales o cualquier otro caso de fuerza mayor.
- Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente PC / DPC y sus Anexos.
- Por el uso indebido o fraudulento de los certificados o CRL's emitidos por la Entidad de Certificación.
- Por el uso de la información contenida en el Certificado o en la CRL.
- Por el incumplimiento de las obligaciones establecidas para el Titular o Terceros que confían en la normativa vigente, la presente PC / DPC y sus Anexos.
- Por el perjuicio causado en el periodo de verificación de las causas de revocación /suspensión.
- Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
- Por la no recuperación de documentos cifrados con la clave pública del Titular.
- Fraude en la documentación presentada por el solicitante.

## 32.4. RESPONSABILIDADES FINANCIERAS

### 32.4.1. COBERTURA DEL SEGURO

Para la EC Raíz, ECs emisoras y los servicios de certificación prestados directamente por emSign, se mantiene un contrato de seguro que cubra la responsabilidad expresada en la sección Obligaciones. Para los afiliados y clientes corporativos que actúan como ECs o ERs, las condiciones contractuales acordadas entre las partes garantizan las responsabilidades asumidas por cada parte y transfieren los requisitos a favor del correspondiente seguro para las obligaciones transferidas.

### 32.4.2. OTROS BIENES

Sin estipulación.

### 32.4.3. SEGURO O GARANTÍA DE COBERTURA PARA LAS ENTIDADES FINALES

La responsabilidad máxima por certificado de la EC Raíz o cualquier otra entidad dentro de su jerarquía se establecerá en la Política de certificación. Dicho límite de responsabilidad por certificado se aplicará con independencia del número de transacciones, firmas digitales, o causas de acción que surjan de ello o esté relacionada con dicho certificado o cualquier servicio proporcionado en relación con dicho certificado y en forma acumulada.

## 32.5. CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

### 32.5.1. ÁMBITO DE LA INFORMACIÓN CONFIDENCIAL

emSign PKI considera la siguiente información como información confidencial y los protege de la divulgación utilizando un grado razonable de atención:

1. Claves privadas;
2. Datos de activación utilizados para acceder a las claves privadas o para obtener acceso al sistema de CA;
3. Planes de continuidad del negocio, respuesta a incidentes, contingencia y recuperación de desastres;
4. Otras prácticas de seguridad utilizadas para proteger la confidencialidad, integridad o disponibilidad de información;

5. Información mantenida por emSign PKI como información privada de acuerdo con este CP / CPS;
6. Auditoría de registros y registros de archivo; y
7. Registros de transacciones, registros de auditoría financiera y registros de seguimiento de auditoría externa o interna y cualquier informe de auditoría (con la excepción de una carta del auditor que confirme la efectividad de los controles establecidos en este CPS).
8. Cualquier otra información relacionada con el suscriptor o emSign PKI, que puede ser de naturaleza confidencial.

#### 32.5.2. INFORMACIÓN NO CONFIDENCIAL

Cualquier información que no sea la información indicada como confidencial en este documento se considerará pública. La información adicional que aparece en los certificados y en el repositorio se considera pública.

#### 32.5.3. DEBER DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

Los empleados, agentes y contratistas de emSign PKI están obligados contractualmente a proteger la información confidencial. Además, enSign brinda capacitación a los empleados sobre la protección de la información confidencial.

## 32.6. PROTECCIÓN DE LA INFORMACIÓN PERSONAL

#### 32.6.1. POLÍTICA DE PRIVACIDAD

emSign PKI y SoftNet protegen la información personal según la Política de privacidad publicada en el Repositorio de ambos.

#### 32.6.2. INFORMACIÓN TRATADA COMO PRIVADA

emSign PKI y SoftNet tratan toda la información personal sobre un solicitante que no está disponible públicamente en el contenido de un Certificado o CRL.

#### 32.6.3. INFORMACIÓN NO CALIFICADA COMO PRIVADA

El contenido del certificado y la información del estado del certificado no se consideran privados en emSign PKI.

#### 32.6.4. RESPONSABILIDAD DE LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL

emSign PKI almacenará información privada de acuerdo con el documento de Política de Privacidad publicado en el repositorio de emSign. Toda la información privada se almacena de forma segura y se protege contra la divulgación accidental.

#### 32.6.5. NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR DATOS DE CARÁCTER PERSONAL

La información personal obtenida de un solicitante durante el proceso de solicitud o verificación de identidad, en la medida en que no se incluya en un certificado, se considera información privada. Dicha información privada será utilizada por emSign y SoftNet solo después de obtener el consentimiento del sujeto o según lo exija la ley o regulación aplicable. Se considera que todos los suscriptores han dado su consentimiento para la transferencia y publicación global de cualquier información personal contenida en un Certificado.

#### 32.6.6. REVELACIÓN EN EL MARCO DE UN PROCESO ADMINISTRATIVO O JUDICIAL

SoftNet pueden divulgar información privada sin previo aviso a los solicitantes o suscriptores cuando dicha divulgación sea requerida por ley o regulación.

#### 32.6.7. OTRAS CIRCUNSTANCIAS DE REVELACIÓN DE INFORMACIÓN

No se estipula.

## 32.7. DERECHOS DE PROPIEDAD INTELECTUAL

emSign y SoftNet no violan a sabiendas los derechos de propiedad intelectual de terceros.
Todos los derechos de propiedad intelectual, incluidos todos los derechos de autor en todos los certificados, todos los documentos, incluido la CP / CPS de emSign, respecto del cual se basa este documento, y todas las marcas registradas pertenecen y seguirán siendo propiedad de eMudhra. eMudhra se reserva el derecho exclusivo de usar y licenciar su propiedad intelectual.
Los certificados son propiedad exclusiva de emSign PKI y SoftNet. Dan permiso para reproducir y distribuir Certificados de forma gratuita, no exclusiva, siempre que se reproduzcan y distribuyan en su totalidad.
emSign PKI y SoftNet se reservan el derecho de revocar un Certificado en cualquier momento y a su exclusivo criterio.
Las claves públicas y las claves privadas son propiedad de los titulares de certificados correspondientes que las poseen legítimamente.
emSign excluye toda responsabilidad por incumplimiento de cualquier otro derecho de propiedad intelectual.

## 32.8. REPRESENTACIONES Y GARANTÍAS

#### 32.8.1. REPRESENTACIÓN DE LA EC Y GARANTÍAS

emSign PKI, como proveedor de servicios de certificación de SoftNet, representa, en la medida especificada en su CP / CPS, emSign PKI cumple, en todos los aspectos materiales, con el CP / CPS y todas las leyes y regulaciones aplicables.
emSign PKI y SoftNet garantizan además que:

1. Han tomado medidas razonables para verificar que la información contenida en cualquier Certificado sea precisa en el momento de la emisión y se verifique de acuerdo con este documento y los requisitos de referencia y las pautas de EV.
2. Los certificados se revocarán si emSign o SoftNet creen o se les notifica que el contenido del certificado ya no es exacto, o que la clave asociada con un certificado se ha visto comprometida de alguna manera.

emSign PKI también proporciona representaciones y garantías como se especifica en los Requisitos de línea de base del CA Browser Forum.
Para los certificados SSL EV, emSign PKI también proporciona representaciones y garantías como se especifica en las Pautas del CA Browser Forum para SSL EV.
emSign no ofrece otras garantías, y todas las garantías, expresas o implícitas, legales o de otro tipo, están excluidas en la mayor medida permitida por la ley aplicable, incluidas, entre otras, todas las garantías en cuanto a comerciabilidad o idoneidad para un propósito particular.

#### 32.8.2. REPRESENTACIÓN Y GARANTÍAS DE LAS ER

Las ER garantizan que:

1. Llevan a cabo el proceso de emisión de conformidad con este documento.

2. La información proporcionada por ellos no contiene ninguna información falsa o engañosa.
3. Todos los certificados solicitados por ellos cumplen con todos los requisitos materiales de este documento.

Las representaciones y garantías adicionales pueden estar contenidas en el acuerdo de SoftNet con las ER asociadas.

### 32.8.3. REPRESENTACIÓN Y GARANTÍAS DEL SUSCRIPTOR

Los suscriptores representan y garantizan a emSign PKI y SoftNet, a los terceros que confían y otras partes que, para cada certificado, el suscriptor:

1. Genere de forma segura sus claves privadas y proteja sus claves privadas del compromiso,
2. Proporcione información precisa y completa cuando se comunique con SoftNet,
3. Confirme la exactitud de los datos del certificado antes de usar el Certificado,
4. Solicite de inmediato la revocación de un Certificado, deje de usarlo y su Clave Privada asociada y notifique a SoftNet si hay algún uso o compromiso real o sospechoso de la Clave Privada asociada con la Clave Pública incluida en el certificado,
5. Solicitar inmediatamente la revocación del Certificado y dejar de usarlo, si alguna información en el Certificado es o se vuelve incorrecta o inexacta,
6. Use el Certificado solo para fines autorizados y legales, de acuerdo con el propósito del certificado, este CPS, cualquier CP aplicable y el Acuerdo de Suscriptor relevante, incluida la instalación de Certificados SSL en servidores accesibles en el dominio que figura en el Certificado y no utilizando el código firmar certificados para firmar código malicioso o cualquier código que se descargue sin el consentimiento del usuario, y
7. Deje de usar el Certificado y la Clave privada relacionada inmediatamente después de la fecha de vencimiento del Certificado.

Los suscriptores representan y garantizan según lo especificado en los requisitos y pautas del CA Browser Forum.

### 32.8.4. REPRESENTACIÓN Y GARANTÍAS DEL TERCERO QUE CONFÍA

El tercero que confía es la única responsable de tomar la decisión de confiar en un certificado SoftNet. Un tercero que confía acepta que para confiar razonablemente en un Certificado de SoftNet, debe asegurarse que:

1. Obtuvo suficiente conocimiento sobre el uso de certificados digitales y PKI,
2. Estudió las limitaciones aplicables en el uso de Certificados y acepta las limitaciones de emSign sobre la responsabilidad relacionada con el uso de Certificados,
3. Leyó, entendió y aceptó el Acuerdo de la Parte Confiable de SoftNet y este documento,
4. Verificó tanto el Certificado SoftNet como los Certificados en la cadena de certificados utilizando la CRL u OCSP relevante
5. No se utilizó un Certificado SoftNet que haya expirado o haya sido revocado,
6. Tomó todas las medidas razonables para minimizar el riesgo asociado con confiar en un certificado de firma digital después de considerar:
    a) la ley aplicable y los requisitos legales para la identificación de una parte, la protección de la confidencialidad o privacidad de la información y la exigibilidad de la transacción;
    b) el uso previsto del Certificado tal como figura en el certificado o en esta DPC,
    c) los datos enumerados en el Certificado,
    d) el valor económico de la transacción o comunicación,
    e) la posible pérdida o daño que podría causar una identificación errónea o una pérdida de confidencialidad o privacidad de la información en la aplicación, transacción o comunicación,

f) el resultado de una negociación previa con el suscriptor para el tercero que confía,
g) la comprensión del comercio del tercero que confía, incluida la experiencia con métodos de comercio basados en computadora, y
h) cualquier otro indicio de confiabilidad o falta de confiabilidad perteneciente al Suscriptor y / o la aplicación, comunicación o transacción.

Cualquier relación de confianza no autorizada de un Certificado es bajo el propio riesgo del tercero que confía.

#### 32.8.5. REPRESENTACIÓN Y GARANTÍAS DE OTRAS PARTES

Sin estipulación

## 32.9. DESCARGO DE RESPONSABILIDAD DE GARANTÍAS

SoftNet por la presente renuncia a todas las garantías, incluida la garantía de comerciabilidad y / o idoneidad para un propósito particular que no sea en la medida prohibida por la ley o expresamente estipulada en este PC y DPC.

## 32.10. RESPONSABILIDAD DE LA AUTORIDAD DE CERTIFICACIÓN

La EC de SoftNet, como EC emisora bajo emSign PKI, proporciona el servicio con el mejor esfuerzo. La seguridad y la idoneidad del servicio no estarán garantizadas por las CA emisoras bajo emSign PKI.
La EC de SoftNet no será responsable por la demora u omisión de emitir / revocar / activar un certificado digital o cualquier otra consecuencia que surja de eventos fuera del control de la EC de SoftNet. SoftNet no será responsable, por ningún certificado obtenido de ella, al representar información falsa o inexacta o engañosa o falsa.
Todas las garantías y exenciones de responsabilidad de los mismos, y cualquier limitación de responsabilidad entre la EC de SoftNet, sus intermediarios (ER / socios) y sus respectivos clientes deberán cumplir estrictamente los términos y condiciones del Acuerdo entre ellos.

#### 32.10.1. LIMITACIÓN DE RESPONSABILIDAD

En la medida en que la EC de SoftNet, como EC emisora bajo emSign PKI, haya emitido y administrado el certificado de acuerdo con la CP / CPS de emSign PKI, no tendrá ninguna responsabilidad ante el Suscriptor, el tercero que confía o cualquier Tercero por cualquier pérdida o daño sufrido como resultado del uso o dependencia de dicho certificado.
La EC de SoftNet será responsable ante los titulares de certificados o los terceros que confían por pérdidas directas derivadas de cualquier incumplimiento de esta PC y DPC o por cualquier otra responsabilidad en la que puedan incurrir en un contrato, agravio u otro, incluida la responsabilidad por negligencia por suscriptor o tercero de confianza o tercero por certificado, siempre que el suscriptor, el tercero de confianza o el tercero cumplan plenamente con dicho PC y DPC.
La responsabilidad de la EC de SoftNet, como EC emisora bajo emSign PKI, a cualquier persona por daños que surjan bajo, fuera o relacionado con esta PC y DPC, Acuerdo de Suscriptor, contrato aplicable o cualquier otro acuerdo relacionado, ya sea por contrato, garantía, agravio o de otro modo, se limitará a los daños reales sufridos por esa persona. La EC de SoftNet no será responsable por daños indirectos, consecuentes, incidentales, especiales, ejemplares o punitivos con respecto a cualquier persona, incluso si se ha informado a emSign PKI de la posibilidad de tales daños, independientemente de cómo dichos daños o responsabilidad puede surgir, ya sea en agravio, negligencia, equidad, contrato, estatuto, derecho consuetudinario o de otra manera.
Al participar dentro de las EC emisoras bajo emSign PKI, cualquier persona que participe dentro de emSign PKI acuerda irrevocablemente que no solicitará ni buscará daños indirectos, ejemplares,

consecuentes, especiales, incidentales o punitivos y confirma irrevocablemente a las EC emisoras bajo emSign PKI su aceptación de lo anterior y el hecho de que emSign ha confiado en lo anterior como una condición e incentivo para permitir que esa persona participe en la Infraestructura de clave pública de emSign.

## 32.11. TÉRMINO Y TERMINACIÓN

### 32.11.1. TÉRMINO

Este PC y DPC y cualquier enmienda a este entrarán en vigencia luego de su publicación en el repositorio de SoftNet y permanecerán vigentes hasta que sea reemplazado por una versión más nueva.

### 32.11.2. TERMINACIÓN

Este CP y DPC y cualquier enmienda permanecerán en vigor hasta que se modifique o reemplace por una versión más nueva.

### 32.11.3. EFECTO DE LA TERMINACIÓN Y LA SUPERVIVENCIA

Al finalizar esta DPC, los participantes de SoftNet están sujetos a sus términos para todos los certificados emitidos por el resto de los períodos de validez de dichos certificados. Como mínimo, todas las responsabilidades relacionadas con la protección de la información confidencial sobrevivirán a la terminación.

## 32.12. AVISOS INDIVIDUALES Y COMUNICACIONES CON LOS PARTICIPANTES

SoftNet acepta avisos relacionados con esta CP y DPC, en papel o en forma electrónica, en la ubicación y / o dirección de correo electrónico especificada en este documento. Los avisos se consideran efectivos después de que el remitente recibe un acuse de recibo válido y firmado de SoftNet. Si el remitente no recibe un acuse de recibo dentro de los siete días, el remitente debe reenviar el aviso en papel a la dirección especificada en este PC y DPC utilizando un servicio de mensajería que confirma la entrega.
SoftNet proporcionará cualquier aviso requerido bajo esta PC y DPC por medios físicos o electrónicos, a menos que se acuerde específicamente lo contrario.

## 32.13. ENMIENDAS

### 32.13.1. PROCEDIMIENTO DE ENMIENDA

Las enmiendas a esta PC y DPC son aprobadas por SoftNet. Tras cualquier modificación, la PCy DPC modificada se publicará en el repositorio en línea dentro de la duración definida en esta PC y DPC.

### 32.13.2. MECANISMO DE NOTIFICACIÓN Y PERÍODO

SoftNet puede hacer cambios a este PC y DPC sin previo aviso y sin cambiar el número de versión; Además, SoftNet no garantiza ni establece un período de notificación y comentarios.

### 32.13.3. CIRCUNSTANCIAS BAJO LAS CUALES SE DEBE CAMBIAR EL OID

Sin estipulación.

## 32.14. PROCEDIMIENTOS DE RESOLUCIÓN DE DISPUTAS

Si surge una disputa entre las partes que participan en la PKI de SoftNet, las partes primero intentarán resolver la disputa mediante negociaciones de buena fe remitiéndose directamente a SoftNet, antes de recurrir a cualquier otro mecanismo de resolución de disputas. Si tales negociaciones de buena fe fracasan, las partes pueden remitir el asunto a arbitraje o adjudicación.

## 32.15. LEY QUE RIGE

Este PC y DPC se rige por las leyes del Perú. La construcción e interpretación de este DPC se realizará de conformidad con las leyes del Perú. El lugar con respecto a cualquier disputa será en Lima, Perú o en cualquier lugar acordado explícitamente con el suscriptor / parte de confianza / cualquier otro acuerdo de parte para el certificado con referencia al que surge la disputa.

## 32.16. CUMPLIMIENTO DE LA LEY APLICABLE

Los certificados emitidos bajo SoftNet serán utilizados por los suscriptores y las partes confiantes solo de acuerdo con las leyes y reglamentos de la jurisdicción en la que se utilizan o se basan. Las CA emisoras bajo emSign PKI pueden negarse a emitir o revocar Certificados si, en su opinión, la emisión o el uso continuado de los Certificados emSign PKI violarían las leyes o regulaciones aplicables.

## 32.17. OTRAS DISPOSICIONES

### 32.17.1. ACUERDO COMPLETO

Sin estipulación

### 32.17.2. ASIGNACIÓN

Las CA emisoras, los suscriptores, las partes confiantes, las Entidades de registro o cualquier otra entidad que opere bajo esta PC y DPC no tienen derecho a asignar ninguno de sus derechos u obligaciones bajo este PC y DPC sin el consentimiento previo por escrito de SoftNet.

### 32.17.3. DIVISIBILIDAD

Si alguna de las disposiciones de esta PC y DPC se considera inválida por una autoridad competente en la jurisdicción aplicable, el resto de la PC y DPC seguirá siendo válido y exigible.

### 32.17.4. CUMPLIMIENTO (RENUNCIA DE DERECHOS)

Las EC emisoras bajo emSign PKI pueden solicitar indemnización y honorarios de abogados de una parte por daños, pérdidas y gastos relacionados con la conducta de esa parte.
Ninguna renuncia a ninguna de las partes será efectiva a menos que sea otorgada por escrito por las CA emisoras respectivas bajo emSign PKI.
En sus acuerdos específicos con suscriptores, las partes confiantes o cualquier otra parte SoftNet puede aceptar otras disposiciones relacionadas con la aplicación.

### 32.17.5. FUERZA MAYOR

SoftNet no acepta ninguna responsabilidad por cualquier retraso o incumplimiento de una obligación en virtud de su PC y DPC en la medida en que dicho retraso o incumplimiento sea causado por eventos que escapen a su control razonable.

## 32.18. OTRAS PROVISIONES

Sin estipulación.

# 33. ANEXO A: REQUISITOS DE VERIFICACIÓN PARA EL SUSCRIPTOR

## 33.1. CERTIFICADO DE CLIENTE - CLASE 1

| | |
|---|---|
| **Uso/Propósito** | Certificado para firma de email con o sin información de identidad |
| **Verificación física** | No estipulado |
| **Verificación del individuo** | Para el individuo validado, la verificación de la identidad y la dirección del solicitante se realizará utilizando una o más de las siguientes validaciones:<br>1. La identidad y la dirección del solicitante se verificarán mediante la obtención de una copia legible, que muestre notablemente la cara del solicitante, de al menos una documento de identificación vigente con foto emitida por el gobierno (pasaporte, documento de identificación nacional, licencia de conducir, identificación de empleo del gobierno o cualquier otro tipo de documento equivalente) o en caso de ser extranjero, carné de extranjería. La copia del documento será inspeccionada por cualquier indicación de alteración o falsificación.<br>2. La identidad del solicitante debe ser verificada:<br>a) En el caso de ciudadanos peruanos, por las bases de datos del RENIEC o el sistema de verificación biométrica AFIS.<br>b) En el caso de extranjeros, por las bases de datos de Migraciones<br>3. Si la dirección no es parte de la prueba de identidad y/o requiere alguna garantía adicional, esto puede verificarse tomando una forma adicional de identificación, como facturas de servicios públicos recientes, facturas telefónicas, estados de cuentas financieras, tarjeta de crédito, una prueba de identificación adicional, o cualquier otro tipo de documento equivalente.<br>4. Se pueden realizar verificaciones cruzadas adicionales del nombre y la dirección del Solicitante para mantener la coherencia con una Fuente de datos confiable.<br>5. Se puede tomar la confirmación de que el Solicitante puede recibir comunicación por teléfono, correo postal / correo o fax.<br>6. Si la verificación no se logra satisfactoriamente por alguno de los procesos anteriores o es necesario un proceso alternativo, puede completarse mediante la aceptación de una Declaración de identidad, atestiguada por la ER, el Agente de confianza o un notario.<br>7. Como una validación alternativa o adicional, se considerará la información sobre la identidad y la dirección de una fuente previamente verificada, incluyendo identificación nacional, identificación del gobierno, información verificada del banco o de telecomunicaciones, o cualquier otra fuente confiable equivalente. |

| | |
|---|---|
| **Verificación de Organización** | Si la Organización debe estar presente en el valor O del certificado, la verificación de la identidad y la dirección del solicitante se realizará utilizando una o más de las siguientes validaciones:<br>1. El Representante Legal o una persona asignada por él deberá acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva.<br>2. El solicitante de los certificados deberá acreditar, mediante el documento legal respectivo o consulta a la base de datos respectiva, sus facultades como representante.<br>3. La identidad de la persona jurídica debe ser verificada:<br>• En el caso de empresas con domicilio en Perú, la existencia y vigencia de la persona jurídica deberá acreditarse con el documento o consulta electrónica de vigencia emitidos por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente, se debe verificar también mediante la base de datos de SUNAT que el RUC se encuentre activo y habido.<br>• En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente o consulta en línea expedida por la autoridad competente en su país de origen.<br>4. La solicitud de certificados por parte de la persona jurídica debe ser realizada por medios no repudiables.<br>5. El representante autorizado, cuya identidad haya sido validada por la ER, designará a los suscriptores que recibirán certificados digitales en nombre de la persona jurídica, por medios no repudiables. |
| **Verificación de número de teléfono** | Si el teléfono debe estar presente en el certificado, el número de teléfono deberá<br>1. Sea parte de una fuente previamente verificada, incluida información verificada por el banco, etc.<br>2. O, verifíquese enviando un mensaje de texto SMS de respuesta de desafío o grabando la voz del solicitante durante una comunicación a / por ese número de teléfono. |
| **Verificación de email** | Si el correo electrónico debe estar presente en el certificado, el control sobre el correo electrónico o el nombre de dominio del servidor de correo electrónico se verificará en la forma de entrega y aceptación del correo electrónico. |

## 33.2. CERTIFICADO DE CLIENTE - CLASE 2

| | |
|---|---|
| **Uso/Propósito** | Firma de documentos / Cifrado / Ambos<br>Para Individuo / Organización Individual / Organización (Certificado de firmante de documento) |
| **Verificación física** | Cara a cara en forma de carta de verificación física por agentes de confianza como notario público. |
| **Verificación del individuo** | Para el individuo validado, la verificación de la identidad y la dirección del solicitante se realizará utilizando una o más de las siguientes validaciones:<br>1. La identidad y la dirección del solicitante se verificarán mediante la obtención de una copia legible, que muestre notablemente la cara del solicitante, de al menos un doumento de identificación vigente con foto emitida por el gobierno (pasaporte, documento de identificación nacional, licencia de conducir, identificación de empleo del gobierno o cualquier otro tipo de documento equivalente) o en caso de ser extranjero, carné de extranjería. La copia del documento será inspeccionada por cualquier indicación de alteración o falsificación.<br>2. La identidad del solicitante debe ser verificada:<br>a) En el caso de ciudadanos peruanos, por las bases de datos del RENIEC o el sistema de verificación biométrica AFIS.<br>b) En el caso de extranjeros, por las bases de datos de Migraciones<br>3. Si la dirección no es parte de la prueba de identidad y/o requiere alguna garantía adicional, esto puede verificarse tomando una forma adicional de identificación, como facturas de servicios públicos recientes, facturas telefónicas, estados de cuentas financieras, tarjeta de crédito, una prueba de identificación adicional, o cualquier otro tipo de documento equivalente.<br>4. Se pueden realizar verificaciones cruzadas adicionales del nombre y la dirección del Solicitante para mantener la coherencia con una Fuente de datos confiable.<br>5. Se puede tomar la confirmación de que el Solicitante puede recibir comunicación por teléfono, correo postal / correo o fax.<br>6. Si la verificación no se logra satisfactoriamente por cualquiera de los procesos anteriores o si es necesario un proceso alternativo, puede completarse aceptando una Declaración de identidad, que esté certificada por la ER, el Agente de confianza o un notario.<br>7. Como una validación alternativa o adicional, se considerará la información sobre la identidad y la dirección de una fuente previamente verificada, incluyendo identificación nacional, identificación del gobierno, información verificada del banco o de telecomunicaciones, o cualquier otra fuente confiable equivalente. |
| **Verificación de la organización** | Si la Organización debe estar presente en el valor O del certificado, la verificación de la identidad y la dirección del solicitante se realizará utilizando una o más de las siguientes validaciones:<br>1. El Representante Legal o una persona asignada por él deberá acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva.<br>2. El solicitante de los certificados deberá acreditar, mediante el documento legal respectivo o consulta a la base de datos respectiva, sus facultades como representante.<br>3. La identidad de la persona jurídica debe ser verificada: |

| | |
|---|---|
| | • En el caso de empresas con domicilio en Perú, la existencia y vigencia de la persona jurídica deberá acreditarse con el documento o consulta electrónica de vigencia emitidos por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente, se debe verificar también mediante la base de datos de SUNAT que el RUC se encuentre activo y habido.<br>• En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente o consulta en línea expedida por la autoridad competente en su país de origen.<br>4. La solicitud de certificados por parte de la persona jurídica debe ser realizada por medios no repudiables.<br>5. El representante autorizado, cuya identidad haya sido validada por la ER, designará a los suscriptores que recibirán certificados digitales en nombre de la persona jurídica, por medios no repudiables. |
| **Verificación de número de teléfono** | Si el teléfono debe estar presente en el certificado, el número de teléfono deberá<br>1. Sea parte de una fuente previamente verificada, incluida información verificada por el banco, etc.<br>2. O, verifíquese enviando un mensaje de texto SMS de respuesta de desafío o grabando la voz del solicitante durante una comunicación a / por ese número de teléfono. |
| **Verificación de email** | Si el correo electrónico debe estar presente en el certificado, el control sobre el correo electrónico o el nombre de dominio del servidor de correo electrónico se verificará en la forma de entrega y aceptación del correo electrónico. |
| **Verificación de Almacén de Llave** | Verificación del almacenamiento de claves en Crypto Hardware (FIPS 140-2 Nivel 2+ o Criterios comunes equivalentes o especificaciones QSCD) por medio de una carta certificada por la organización, o visita al sitio, o hardware administrado / operado por CA o un tercero de confianza. El control clave con el suscriptor también puede verificarse de esa manera. |

## 33.3. CERTIFICADO DE CLIENTE - CLASE 3

| | |
|---|---|
| **Uso/Propósito** | Firma de documentos / Cifrado / Ambos<br>Para Individuo / Organización Individual / Organización (Certificado de firmante de documento) |
| **Verificación física** | Verificación cara a cara por ER |
| **Verificación del individuo** | Para el individuo validado, la verificación de la identidad y la dirección del solicitante se realizará utilizando una o más de las siguientes validaciones:<br>1. La identidad y la dirección del solicitante se verificarán mediante la obtención de una copia legible, que muestre notablemente la cara del solicitante, de al menos un doumento de identificación vigente con foto emitida por el gobierno (pasaporte, documento de identificación nacional, licencia de conducir, identificación de empleo del gobierno o cualquier otro tipo de documento equivalente) o en caso de ser extranjero, carné de extranjería. La copia del documento será inspeccionada por cualquier indicación de alteración o falsificación.<br>2. La identidad del solicitante debe ser verificada:<br>a) En el caso de ciudadanos peruanos, por las bases de datos del RENIEC o el sistema de verificación biométrica AFIS.<br>b) En el caso de extranjeros, por las bases de datos de Migraciones<br>3. Si la dirección no es parte de la prueba de identidad y/o requiere alguna garantía adicional, esto puede verificarse tomando una forma adicional de identificación, como facturas de servicios públicos recientes, facturas telefónicas, estados de cuentas financieras, tarjeta de crédito, una prueba de identificación adicional, o cualquier otro tipo de documento equivalente.<br>4. Se pueden realizar verificaciones cruzadas adicionales del nombre y la dirección del Solicitante para mantener la coherencia con una Fuente de datos confiable.<br>5. Se puede tomar la confirmación de que el Solicitante puede recibir comunicación por teléfono, correo postal / correo o fax.<br>6. Si la verificación no se logra satisfactoriamente por cualquiera de los procesos anteriores o si es necesario un proceso alternativo, puede completarse aceptando una Declaración de identidad, que esté certificada por la ER, el Agente de confianza o un notario.<br>7. Como una validación alternativa o adicional, se considerará la información sobre la identidad y la dirección de una fuente previamente verificada, incluyendo identificación nacional, identificación del gobierno, información verificada del banco o de telecomunicaciones, o cualquier otra fuente confiable equivalente. |

| | |
|---|---|
| **Verificación de la organización** | Si la Organización debe estar presente en el valor O del certificado, la verificación de la identidad y la dirección del solicitante se realizará utilizando una o más de las siguientes validaciones:<br>1. El Representante Legal o una persona asignada por él deberá acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva.<br>2. El solicitante de los certificados deberá acreditar, mediante el documento legal respectivo o consulta a la base de datos respectiva, sus facultades como representante.<br>3. La identidad de la persona jurídica debe ser verificada:<br>• En el caso de empresas con domicilio en Perú, la existencia y vigencia de la persona jurídica deberá acreditarse con el documento o consulta electrónica de vigencia emitidos por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente, se debe verificar también mediante la base de datos de SUNAT que el RUC se encuentre activo y habido.<br>• En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente o consulta en línea expedida por la autoridad competente en su país de origen.<br>4. La solicitud de certificados por parte de la persona jurídica debe ser realizada por medios no repudiables.<br>5. El representante autorizado, cuya identidad haya sido validada por la ER, designará a los suscriptores que recibirán certificados digitales en nombre de la persona jurídica, por medios no repudiables. |
| **Verificación de número de teléfono** | Si el teléfono debe estar presente en el certificado, el número de teléfono deberá<br>1. Sea parte de una fuente previamente verificada, incluida información verificada por el banco, etc.<br>2. O, verifíquese enviando un mensaje de texto SMS de respuesta de desafío o grabando la voz del solicitante durante una comunicación a / por ese número de teléfono. |
| **Verificación de email** | Si el correo electrónico debe estar presente en el certificado, el control sobre el correo electrónico o el nombre de dominio del servidor de correo electrónico se verificará en la forma de entrega y aceptación del correo electrónico. |
| **Verificación de Almacén de Llave** | Verificación del almacenamiento de claves en Crypto Hardware (FIPS 140-2 Nivel 2+ o Criterios comunes equivalentes o especificaciones QSCD) por medio de una carta certificada por la organización, o visita al sitio, o hardware administrado / operado por CA o un tercero de confianza. El control clave con el suscriptor también puede verificarse de esa manera. |

# 34. ANEXO B: PERFILES DE CERTIFICADO

## 34.1. CERTIFICADOS RAIZ

| | |
|---|---|
| Version | V3 |
| Serial Number | Unique Non-Sequential CSPRNG Number and is greater than zero. |
| Signature Algorithm | SHA-256, SHA-384 or SHA-512 with RSA Encryption or<br>ECDSA with SHA-256, SHA-384 or SHA-512 |
| Issuer: CN | <Issuing CA Common Name> |
| Issuer: O | <Issuing CA Organization name> |
| Issuer: OU | <Issuing CA Organization unit> |
| Issuer: C | <Issuing CA Country> |
| Valid From | Start date expressed in UTC format |
| Valid To | Start date expressed in UTC format |
| Public Key | RSA 2048 (OR)<br>ECC curves NIST P-256, P-384, or P-521 |
| Subject: CommonName | Common Name of Root CA |
| Subject: OrganizationName | Legal Name of CA Organization |
| Subject: OrganizationalUnitName | Variable Information |
| Subject: CountryName | Country of CA |
| Key Usage | Critical=TRUE<br>Certificate Signing, Off-line CRL Signing, CRL Signing (06) |
| Subject Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Basic Constraints | Critical=TRUE<br>Subject Type=CA, Path Length Constraint=None |

## 34.2. CERTIFICADOS DE EC SUBORDINADA (EMISOR / INTERMEDIA)

| | |
|---|---|
| Version | V3 |
| Serial Number | Unique Non-Sequential CSPRNG Number and is greater than zero. |
| Signature Algorithm | SHA-256, SHA-384 or SHA-512 with RSA Encryption or<br>ECDSA with SHA-256, SHA-384 or SHA-512 |
| Issuer: CN | <Issuing CA Common Name> |
| Issuer: O | <Issuing CA Organization name> |
| Issuer: OU | <Issuing CA Organization unit> |
| Issuer: C | <Issuing CA Country> |
| Valid From | Start date expressed in UTC format |
| Valid To | Start date expressed in UTC format |
| Public Key | RSA 2048 (OR)<br>ECC curves NIST P-256, P-384, or P-521 |
| Subject: CommonName | Common Name of CA |
| Subject: OrganizationName | Legal Name of CA Organization |
| Subject: OrganizationalUnitName | Variable Information |
| Subject: CountryName | Country of CA |
| Key Usage | Critical=TRUE<br>Certificate Signing, Off-line CRL Signing, CRL Signing (06) |
| Enhanced Key Usage | In case the CA issues Server Authentication certificates: |
| | Critical=FALSE<br>Server Authentication, Client Authentication<br><br>In case the CA issues Code Signing certificates:<br>Code Signing<br><br>In other cases, it will not be present or limits to other 'key usage types' with critical=false. |
| Certificate Policies | Critical=FALSE<br>1. Policy ID=2.5.29.32.0 (CPS, http://repository.emsign.com |
| Subject Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Authority Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Basic Constraints | Critical=TRUE<br>Subject Type=CA, Path Length Constraint=n |
| Authority Information access | Critical=FALSE<br>Access Method=OCSP (1.3.6.1.5.5.7.48.1),<br>URL=http://ocsp.emSign.com |
| CRL Distribution Points | Critical=FALSE<br>CRL HTTP URL = http://crl.emsign.com?<IssuerName>.crl |

### 34.3. CERTIFICADO DE DISPOSITIVO

| | |
|---|---|
| Version | V3 |
| Serial Number | Unique Non-Sequential CSPRNG Number and is greater than zero. |
| Signature Algorithm | SHA-256, SHA-384 or SHA-512 with RSA Encryption or<br>ECDSA with SHA-256, SHA-384 or SHA-512 |
| Issuer: CN | <Issuing CA Common Name> |
| Issuer: O | <Issuing CA Organization name> |
| Issuer: OU | <Issuing CA Organization unit> |
| Issuer: C | <Issuing CA Country> |
| Valid From | Start date expressed in UTC format |
| Valid To | Start date expressed in UTC format |
| Public Key | RSA 2048 (OR)<br>ECC curves NIST P-256, P-384, or P-521 |
| Subject: CommonName | Subject Common Name |
| Subject: GivenName | First name (Optional if Organization name provided) |
| Subject: Surname | Last name (Optional if Organization name provided) |
| Subject: OrganizationName | Organization name (Optional if Individual name provided) |
| Subject: OrganizationalUnitName | Variable Information (optional) |
| Subject: LocalityName | Verified Locality |
| Subject: StateOrProvinceName | Verified State/Province |
| Subject: CountryName | Verified Country |
| Subject Alternative Name | Critical=FALSE<br>RFC822Name = EmailAddress |
| Key Usage | Critical=TRUE<br>Digital Signature, (in case of RSA algorithm, it shall also contain Key Encipherment, Data Encipherment) |
| Enhanced Key Usage | Critical=FALSE<br>Client Authentication, Secure Email |
| Certificate Policies | Critical=FALSE<br>1. Policy ID=1.3.6.1.4.1.50977.1.2.300 (User Notice, Device Certificate)<br>2. Policy ID=1.3.6.1.4.1.50977.1.0.1 (CPS, http://repository.emsign.com |
| Subject Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Authority Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Basic Constraints | Critical=TRUE<br>Subject Type=End Entity, Path Length Constraint=None |
| Authority Information access | Critical=FALSE |

| | |
|---|---|
| | Access Method=OCSP (1.3.6.1.5.5.7.48.1), URL=http://ocsp.emSign.com |
| CRL Distribution Points | Critical=FALSE<br>CRL HTTP URL = http://crl.emsign.com?<IssuerName>.crl |

### 34.4. CERTIFICADOS DE CLIENTE - CLASE 1

| | |
|---|---|
| Version | V3 |
| Serial Number | Unique Non-Sequential CSPRNG Number and is greater than zero. |
| Signature Algorithm | SHA-256, SHA-384 or SHA-512 with RSA Encryption or<br>ECDSA with SHA-256, SHA-384 or SHA-512 |
| Issuer: CN | <Issuing CA Common Name> |
| Issuer: O | <Issuing CA Organization name> |
| Issuer: OU | <Issuing CA Organization unit> |
| Issuer: C | <Issuing CA Country> |
| Valid From | Start date expressed in UTC format |
| Valid To | Start date expressed in UTC format |
| Public Key | RSA 2048 (OR)<br>ECC curves NIST P-256, P-384, or P-521 |
| Subject: CommonName | Common Name |
| Subject: GivenName | First name (Optional if Organization name provided) |
| Subject: Surname | Last name (Optional if Organization name provided) |
| Subject: OrganizationName | Organization name (Optional if Individual name provided) |
| Subject: OrganizationalUnitName | Variable Information (optional) |
| Subject: StreetAddress | Verified Steet address (optional) |
| Subject: LocalityName | Verified Locality (optional) |
| Subject: StateOrProvinceName | Verified State/Province (optional) |
| Subject: CountryName | Verified Country (optional) |
| Subject: PostalCode | Verified Postal Code (optional) |
| Subject: TelephoneNumber | Verified Telephone in SHA256 Hash (optional) |
| Subject: EmailAddress | Verified Email Address |
| Subject Alternative Name | Critical=FALSE<br>RFC822Name = EmailAddress |
| Key Usage | Critical=TRUE<br>digitalSignature, nonRepudiation OR<br>keyEncipherment (in case of RSA) OR<br>digitalSignature, nonRepudiation, keyEncipherment (in case of RSA) |
| Enhanced Key Usage | Critical=FALSE<br>smartcardlogon, clientAuth, emailProtection OR<br>emailProtection OR<br>smartcardlogon, clientAuth, emailProtection |
| Certificate Policies | Critical=FALSE<br>1. Policy ID=1.3.6.1.4.1.50977.1.2.400 (User Notice, Class 1 Client Certificate)<br>2. Policy ID=1.3.6.1.4.1.50977.1.0.1 (CPS, http://repository.emsign.com |

| | |
|---|---|
| Subject Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Authority Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Basic Constraints | Critical=TRUE<br>Subject Type=End Entity, Path Length Constraint=None |
| Authority Information access | Critical=FALSE<br>Access Method=OCSP (1.3.6.1.5.5.7.48.1), URL=http://ocsp.emSign.com |
| CRL Distribution Points | Critical=FALSE<br>CRL HTTP URL = http://crl.emsign.com?<IssuerName>.crl |

### 34.5. CERTIFICADOS DE CLIENTE - CLASE 2

| | |
|---|---|
| Version | V3 |
| Serial Number | Unique Non-Sequential CSPRNG Number and is greater than zero. |
| Signature Algorithm | SHA-256, SHA-384 or SHA-512 with RSA Encryption or<br>ECDSA with SHA-256, SHA-384 or SHA-512 |
| Issuer: CN | <Issuing CA Common Name> |
| Issuer: O | <Issuing CA Organization name> |
| Issuer: OU | <Issuing CA Organization unit> |
| Issuer: C | <Issuing CA Country> |
| Valid From | Start date expressed in UTC format |
| Valid To | Start date expressed in UTC format |
| Public Key | RSA 2048 (OR)<br>ECC curves NIST P-256, P-384, or P-521 |
| Subject: CommonName | Common Name |
| Subject: GivenName | First name (Optional if Organization name provided) |
| Subject: Surname | Last name (Optional if Organization name provided) |
| Subject: OrganizationName | Organization name (Optional if Individual name provided) |
| Subject: OrganizationalUnitName | Variable Information (optional) |
| Subject: StreetAddress | Verified Steet address (optional) |
| Subject: LocalityName | Verified Locality |
| Subject: StateOrProvinceName | Verified State/Province |
| Subject: CountryName | Verified Country |
| Subject: PostalCode | Verified Postal Code (Optional) |
| Subject: TelephoneNumber | Verified Telephone in SHA256 Hash (Optional) |
| Subject: EmailAddress | Verified Email Address (Optional) |
| Subject Alternative Name | Critical=FALSE<br>RFC822Name = EmailAddress |
| Key Usage | Critical=TRUE<br>digitalSignature, nonRepudiation OR<br>keyEncipherment (in case of RSA) |
| | OR<br>digitalSignature, nonRepudiation, keyEncipherment (in case of RSA) |
| Enhanced Key Usage | Critical=FALSE<br>smartcardlogon, clientAuth, emailProtection OR<br>emailProtection OR<br>smartcardlogon, clientAuth, emailProtection |
| Certificate Policies | Critical=FALSE<br>1. Policy ID=1.3.6.1.4.1.50977.1.2.410 (User Notice, Class 2 Client Certificate) |

| | |
|---|---|
| | 2. Policy ID=1.3.6.1.4.1.50977.1.0.1 (CPS, http://repository.emsign.com |
| Subject Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Authority Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Basic Constraints | Critical=TRUE<br>Subject Type=End Entity, Path Length Constraint=None |
| Authority Information access | Critical=FALSE<br>Access Method=OCSP (1.3.6.1.5.5.7.48.1), URL=http://ocsp.emSign.com |
| CRL Distribution Points | Critical=FALSE<br>CRL HTTP URL = http://crl.emsign.com?<IssuerName>.crl |

## 34.6. CERTIFICADOS DE CLIENTE - CLASE 3

| | |
|---|---|
| Version | V3 |
| Serial Number | Unique Non-Sequential CSPRNG Number and is greater than zero. |
| Signature Algorithm | SHA-256, SHA-384 or SHA-512 with RSA Encryption or<br>ECDSA with SHA-256, SHA-384 or SHA-512 |
| Issuer: CN | <Issuing CA Common Name> |
| Issuer: O | <Issuing CA Organization name> |
| Issuer: OU | <Issuing CA Organization unit> |
| Issuer: C | <Issuing CA Country> |
| Valid From | Start date expressed in UTC format |
| Valid To | Start date expressed in UTC format |
| Public Key | RSA 2048 (OR)<br>ECC curves NIST P-256, P-384, or P-521 |
| Subject: CommonName | Common Name |
| Subject: GivenName | First name (Optional if Organization name provided) |
| Subject: Surname | Last name (Optional if Organization name provided) |
| Subject: OrganizationName | Organization name (Optional if Individual name provided) |
| Subject: OrganizationalUnitName | Variable Information (optional) |
| Subject: StreetAddress | Verified Steet address (optional) |
| Subject: LocalityName | Verified Locality |
| Subject: StateOrProvinceName | Verified State/Province |
| Subject: CountryName | Verified Country |
| Subject: PostalCode | Verified Postal Code (Optional) |
| Subject: TelephoneNumber | Verified Telephone in SHA256 Hash (Optional) |
| Subject: EmailAddress | Verified Email Address (Optional) |
| Subject Alternative Name | Critical=FALSE<br>RFC822Name = EmailAddress |
| Key Usage | Critical=TRUE<br>digitalSignature, nonRepudiation OR<br>keyEncipherment (in case of RSA) OR<br>digitalSignature, nonRepudiation, keyEncipherment (in case of RSA) |
| Enhanced Key Usage | Critical=FALSE<br>smartcardlogon, clientAuth, emailProtection OR<br>emailProtection OR<br>smartcardlogon, clientAuth, emailProtection |
| Certificate Policies | Critical=FALSE<br>1. Policy ID=1.3.6.1.4.1.50977.1.2.420 (User Notice, Class 3 Client Certificate)<br>2. Policy ID=1.3.6.1.4.1.50977.1.0.1 (CPS, http://repository.emsign.com |

| | |
|---|---|
| Subject Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Authority Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Basic Constraints | Critical=TRUE<br>Subject Type=End Entity, Path Length Constraint=None |
| Authority Information access | Critical=FALSE<br>Access Method=OCSP (1.3.6.1.5.5.7.48.1), URL=http://ocsp.emSign.com |
| CRL Distribution Points | Critical=FALSE<br>CRL HTTP URL = http://crl.emsign.com?<IssuerName>.crl |

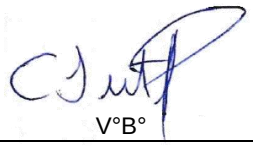
## 34.7. CERTIFICADOS DE TSU

| | |
|---|---|
| Version | V3 |
| Serial Number | Unique Non-Sequential CSPRNG Number and is greater than zero. |
| Signature Algorithm | SHA-256, SHA-384 or SHA-512 with RSA Encryption or<br>ECDSA with SHA-256, SHA-384 or SHA-512 |
| Issuer: CN | <Issuing CA Common Name> |
| Issuer: O | <Issuing CA Organization name> |
| Issuer: OU | <Issuing CA Organization unit> |
| Issuer: C | <Issuing CA Country> |
| Valid From | Start date expressed in UTC format |
| Valid To | Start date expressed in UTC format |
| Public Key | RSA 2048 (OR)<br>ECC curves NIST P-256, P-384, or P-521 |
| Subject: CommonName | Common Name of TSA |
| Subject: OrganizationName | Legal Name of TSA Organization |
| Subject: CountryName | Country of TSA |
| Key Usage | Critical=TRUE<br>nonRepudiation |
| Enhanced Key Usage | Critical=TRUE<br>timeStamping |
| Certificate Policies | Critical=FALSE<br>1. Policy ID=1.3.6.1.4.1.50977.1.2.500 (User Notice, Time Stamping Certificate)<br>2. Policy ID=1.3.6.1.4.1.50977.1.0.1 (CPS, http://repository.emsign.com |
| Subject Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Authority Key Identifier | Critical=FALSE<br>160 bit hash (SHA-1) |
| Basic Constraints | Critical=TRUE<br>Subject Type=End Entity, Path Length Constraint=None |
| Authority Information access | Critical=FALSE<br>Access Method=OCSP (1.3.6.1.5.5.7.48.1), URL=http://ocsp.emSign.com |
| CRL Distribution Points | Critical=FALSE<br>CRL HTTP URL = http://crl.emsign.com?<IssuerName>.crl |

# 35. ANEXO C: HISTORIAL DE CAMBIOS

| ***Generales*** | | | |
|---|---|---|---|
| **Propietario del Documento** | *Carlos Dextre* | Clasificación | *Privada* |
| **Aprobado por:** | *Carlos Dextre* | Fecha aprobación | *12/06/2020* |

| ***Fecha*** | ***Version*** | ***Desripcion*** | ***Autor*** |
|---|---|---|---|
| *12/06/2020* | *1.0* | *Documento Inicial* | *Coordinador de Seguridad de la Información* |
| *12/06/2020* | *1.0* | *Aprobacion* | *Responsable de la EC* |
| *12/06/2020* | *1.0* | *Revision de Documento* | *Gerente de Productos y Servicios* |

| Elaborado por: | Revisado por: | Aprobado por: |
|---|---|---|
|  <br>V°B° |  <br>V°B° |  <br>V°B° |
| Cargo: Coordinador de Seguridad de la Información | Cargo: Gerente de Productos y Servicios | Cargo: Gerente General<br>Responsable de la EC |