DECLARACION DE PRACTICAS DEL SGERE

Firmado Digitalmente por:
PEDRO EMILIO RIVERA PEREZ
Cargo: CISO - GSIG
Fecha: 11/12/2025 07:19:16

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, así como su Entidad de Registro, 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. VISIÓN GENERAL

Esta Declaración de Prácticas de Registro (DPR) presenta los procedimientos y prácticas empleados en el registro y la validación de la identidad de los solicitantes (titulares y suscriptores) de los servicios de emisión y revocación de certificados digitales, esto incluye la verificación de la información entregada por los solicitantes antes de comunicar a la Entidad de Certificación de SOFTNET la aprobación de una solicitud.

2. OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre la infraestructura y procesos de los servicios de registro y verificación de identidad brindados por SOFTNET en el marco del cumplimiento de los requerimientos de la Guía de acreditación de Entidades de Registro o Verificación establecida por INDECOPI.

3. DEFINICIONES Y ABREVIACIONES

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.
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.
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).
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.
Titular de certificado digital	Persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.

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. SOFTNET es una EC bajo la jerarquía de eMudhra, quien es además su proveedor de servicios de certificación, quien cuenta con certificación WebTrust y es miembro de la Adobe Approved Trust List (AATL).
- Cualquier otra Entidad de Certificación acreditada que tiene convenio con la ER de SOFTNET.

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, y como tal presta su infraestructura y servicios tecnológicos a esta entidad de certificación, así como el servicio web de registro (mediante el cual la ER de SOFTNET gestionará la aprobación de las solicitudes de los servicios de certificación digital), 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 CPS o DPC de la EC asociada a 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 o persona designada por éste, 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. ENTIDADES DE CERTIFICACIÓN ASOCIADAS A LA ER DE SOFTNET

A continuación se listan las entidades asociadas a la ER de SOFTNET con convenio vigente a la fecha:

- La EC de SOFTNET, a través de su proveedor de servicios de certificación, ofrece a sus entidades de registro acceso a su plataforma para la gestión del ciclo de vida de los certificados emitidos por ésta.

6. USO DEL CERTIFICADO

6.1. USOS ADECUADOS DEL CERTIFICADO

Los usos adecuados de los certificados emitidos son especificados en las Políticas de Certificación de cada EC asociada a la ER de SOFTNET.

Los certificados emitidos bajo dichas políticas de certificación pueden ser utilizados con los siguientes propósitos:

- 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 Destino 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.

Cada política de certificación está identificada por un único identificador de objeto (OID).

Los tipos de certificados de acuerdo al tipo de titular son los siguientes:

- Certificado para persona natural
- Certificado para persona jurídica
- Certificado para el representante legal
- Certificado de atributo o de pertenencia a empresa
- Certificado de agente automatizado
- Certificado de TSA/TSU

En el caso de la EC de SOFTNET los certificados también se clasifican por el tipo de identificación del suscriptor en:

- Certificados de Clase 1: El proceso de validación de identidad del suscriptor se podrá realizar empleando videollamadas u otro medio no presencial. Sólo se emplearán bajo autorización de la AAC.
- Certificados de Clase 2: El proceso de validación de identidad del suscriptor se realizará por un tercero contratista o por un notario.
- Certificados de Clase 3: El proceso de validación de identidad del suscriptor se realizará de manera presencial por un asistente de validación de identidad o por un operador de registro de la ER de SOFTNET.

Finalmente, el ciclo de vida de un certificado personal no debe exceder el periodo establecido por la IOFE, el mismo que corresponde a máximo de tres (3) años de acuerdo con la legislación vigente.

6.2. USOS PROHIBIDOS DEL CERTIFICADO Y EXCLUSIÓN DE RESPONSABILIDAD

Los certificados sólo podrán ser empleados para los usos para los que hayan sido emitidos y especificados en esta RPS o DPR y concretamente en las Políticas de Certificación de cada EC asociada. Se consideran indebidos aquellos usos que no están definidos en esta RPS o DPR 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 RPS.

7. RESPONSABILIDADES Y OBLIGACIONES

7.1. DE LA ER DE SOFTNET

Son responsabilidades de la ER de SOFTNET:

- Realizar la verificación de identidad de los titulares y suscriptores solicitantes de los certificados digitales, esto implica ejecutar los procedimientos indicados en la presente RPS o DPR para la verificación de la identidad de las personas jurídicas y naturales, según corresponda.
- Garantizar la seguridad y protección de los datos personales y confidenciales recolectados por la ER de SOFTNET, con el propósito de la verificación de identidad de los titulares y suscriptores.
- Garantizar las responsabilidades contractuales, garantías financieras y coberturas de seguros brindadas por la ER de SOFTNET.
- Gestionar la aprobación de las solicitudes de los servicios de certificación digital cuando estos sean solicitados a la ER de SOFTNET.

7.2. DE LOS TITULARES Y SUSCRIPTORES

Los titulares y suscriptores de los certificados digitales provistos a través de la ER de SOFTNET, son responsables de revisar la Política de Certificación de la EC emisora y la presente Declaración de Prácticas y Política de Registro de SOFTNET, 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 las claves privadas de su compromiso.
- Informar inmediatamente 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 el par de claves para la firma digital de acuerdo con el perfil del certificado digital asociado 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 par de claves de conformidad con la Declaración de Prácticas y Política de Certificación de la EC emisora.
- Cualquier otro término indicado en su contrato.

7.3. DE LOS TERCEROS QUE CONFÍAN

Los terceros que confían deben actuar de acuerdo con las obligaciones y responsabilidades establecidas en la CPS de la EC y en los documentos normativos de la Entidad de Registro.
Los terceros que confían pueden verificar el estado de los certificados de acuerdo con lo establecido en el marco de la IOFE. De no hacerlo asumen las consecuencias de dicha omisión.
La documentación normativa de la ER se encuentra publicada en el site de SOFTNET:

www.soft-net.com.pe

7.4. DE LOS TERCEROS CONTRATISTAS

Los terceros contratistas deben actuar de acuerdo con las obligaciones y responsabilidades establecidas en la CPS o DPC de la EC asociada y en los documentos normativos de la ER de SOFTNET.
La ER de SOFTNET garantiza la seguridad y protección de los datos personales y confidenciales de la ER, así como la integridad y autenticidad de las transacciones en la autorización de solicitudes de emisión, o de cancelación (revocación), durante la ejecución de las actividades de tercerización, los cuales están sujetos al cumplimiento de los contratos con los que se vincula a la ER de SOFTNET. En este sentido, la ER tiene previsto tercerizar las funciones de los operadores de registro o de los asistentes de verificación de identidad en terceras entidades, con el fin de que éstas puedan realizar los procesos de validación y/o emisión de los certificados digitales, según el alcance de la tercerización. Para lo cual, se firmará un contrato con dichos terceros en el cual se indicarán las obligaciones de los mismos y los controles de seguridad que éstos deben cumplir, así como indicarse que deben de actuar de acuerdo con las obligaciones y responsabilidades establecidas en la CPS o DPC de la EC asociada y en los documentos normativos de la ER de SOFTNET.

8. 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/

9. ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS NORMATIVOS

SOFTNET administra todos los documentos normativos de su ER, en particular la Declaración de Prácticas de Registro y Política de Registro. Para cualquier consulta contactar con:

Nombre: Leonel José García Jáuregui
Cargo: Director Comercial y de Negocios
email: lgarcia@soft-net.com.pe

10. PUBLICACIÓN DE LOS DOCUMENTOS NORMATIVOS

La Declaración de Prácticas de Registro y Política de Registro, la Política y Plan de Privacidad, la Política de la Seguridad de la Información de la ER 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.

10.1. PROTECCIÓN DE LA INTEGRIDAD DE LOS DOCUMENTOS NORMATIVOS PUBLICADOS

El presente documento y los demás documentos normativos que son publicados son firmados por el Responsable de la ER de SOFTNET antes de ser publicados. Se controla las versiones de los mismos, a fin de evitar modificaciones y suplantaciones no autorizadas.
Los documentos referidos a la CPS o DPC de las EC asociadas también estarán dsponibles desde la dirección indicada o en su defecto redireccionadas a la página de dicha EC.

11. RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

11.1. PUBLICACIÓN DE LA INFORMACIÓN DE CERTIFICACIÓN

El Responsable de la ER de SOFTNET es el encargado de la autorización de la publicación de toda información relevante y pública de la ER y es responsable de asegurar la integridad y disponibilidad de la información publicada en la página web de SOFTNET: http://www.soft-net.com.pe/

11.2. PLAZO O FRECUENCIA DE LA PUBLICACIÓN

Toda documentación relevante y pública de la ER será publicada al día útil siguiente luego de su aprobación por parte del INDECOPI.

11.3. CONTROLES DE ACCESO A LOS REPOSITORIOS

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

12. IDENTIFICACIÓN Y AUTENTICACIÓN

12.1. NOMBRES

12.1.1. TIPOS DE NOMBRES

El documento guía que la EC asociada utiliza para la identificación única de los titulares de certificados emitidos está definido en la estructura de Nombre Distintivo "Distinguished Name (DN)" de la norma ISO/IEC 9595 (X.500).
Los certificados emitidos por la EC asociada contiene el nombre distintivo (distinguished name o DN) X.500 del emisor y el destinatario del certificado en los campos issuer name y subject name respectivamente.

12.1.2. NECESIDAD DE QUE LOS NOMBRES TENGAN SIGNIFICADO

Los nombres distintivos (DN) de los certificados emitidos por la EC asociada son únicos y permiten establecer un vínculo entre la clave pública y el número de identificación del titular.
Debido a que una misma persona o entidad puede solicitar varios certificados a su nombre, estos se diferenciarán por el uso de un valor único en el campo DN. Si se llegase a presentar conflicto sobre la asignación y empleo de un nombre, este será resuelto previo conocimiento por parte de los responsables de estos temas de la EC asociada.

12.1.3. 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.

12.1.4. 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 la EC asociada es el estándar ISO/IEC 9595 (X.500) Distinguished Name (DN).

12.1.5. SINGULARIDAD DE LOS NOMBRES

El DN de los certificados emitidos es único.

12.1.6. RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE MARCAS RECONOCIDAS

La EC asociada 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.

13. SOLICITUD DE EMISIÓN DE CERTIFICADOS DIGITALES

Los procedimientos, requisitos de solicitud y responsabilidades en el uso de los certificados, pueden tener variación de acuerdo con lo establecido en la PC de la EC asociada. Sin embargo, conforme a lo establecido en la normatividad peruana, la ER de SOFTNET realizará como mínimo los siguientes procedimientos de verificación para la validación de la identidad:

13.1. SOLICITUD DE CERTIFICADOS DE PERSONA NATURAL

13.1.1. Servicios brindados

La ER de SOFTNET brinda los siguientes servicios a personas naturales:

a) Atención de solicitudes de emisión de certificados para personas naturales de nacionalidad peruana.
b) Atención de solicitudes de emisión de certificados para personas naturales de nacionalidad extranjera.

13.1.2. Autorizados para realizar la solicitud

La solicitud en el caso de personas naturales debe ser hecha por la misma persona que pretende ser titular del certificado: el solicitante.

13.1.3. Modalidades de atención

La solicitud puede ser realizada mediante un contrato de Prestación de Servicio de Certificación Digital de los certificados digitales que puede ser celebrado de las siguientes formas:

- De manera presencial en las instalaciones de SOFTNET en calidad de ER de la EC asociada.
- De manera presencial en un lugar designado por el solicitante en presencia de un representante de la ER.
- Cuando la persona natural se encuentre en provincia, puede acudir a un notario que certifique la firma del contrato y la identidad del firmante. El contrato deberá ser enviado a las oficinas de SOFTNET.
- De manera virtual, previa verificación de los documentos solicitados ante los entes rectores (RENIEC, Migraciones, otros), se realizara a través de la plataforma de Microsoft que se encuentra debidamente licenciada y que cuenta con los medios de seguridad establecidos por Microsoft a sus servicios, permitirá que a través de una videoconferencia el Operador asignado guie en el proceso de verificación de identidad y de emisión del certificado a través de la plataforma de generación de certificados digitales.

13.1.4. Solicitud de certificados de persona natural

El solicitante deberá realizar su solicitud en cualquiera de las modalidades de atención especificadas en el presente documento, portando el original de un documento oficial de identidad, el mismo que deberá estar en vigor en la fecha de realización del proceso de registro. No se admitirán fotocopias u otro tipo de documento.

13.1.5. Periodo de vigencia de los certificados

En el caso de los certificados de persona natural el periodo de vigencia del certificado solicitado no deberá exceder el periodo de tres (3) años de acuerdo a la legislación vigente.

13.1.6. Contrato del suscriptor

El solicitante deberá firmar un contrato, que en adelante llamaremos "contrato del suscriptor", el cual contiene las obligaciones que deben cumplir el suscriptor o titular del certificado de conformidad con la legislación de la materia para garantizar el efecto legal de las transacciones realizadas, establecidas por las ER de SOFTNET en coordinación con la EC asociada, así como las consecuencias de no cumplir con el acuerdo.
Este contrato deberá ser firmado de manera manuscrita por el solicitante, para luego ser archivado por SOFTNET en calidad de ER de la EC asociada.
A través de dicho contrato, el solicitante deberá declarar tener conocimiento de los términos y condiciones aplicables a los certificados.
La celebración de dicho contrato deberá realizarse antes de la emisión de los certificados.

13.1.7. Verificación de suscriptores

Los aspirantes a suscriptores deben ser validados en cualquiera de las siguientes modalidades:

- De manera presencial en las instalaciones de SOFTNET en calidad de ER de la EC asociada.
- De manera presencial en las instalaciones del cliente, o un lugar designado por éste en presencia de un representante de la ER.
- Cuando el suscriptor se encuentre en provincia, puede acudir a un notario que certifique la firma del contrato y la identidad del firmante. Dicho documento deberá ser enviado a las oficinas de SOFTNET.

13.1.8. Identificación y autenticación de suscriptor

El aspirante a suscriptor debe presentarse en persona ante un funcionario de la ER de SOFTNET portando el original de su documento de identidad, esto es, DNI vigente para personas de nacionalidad peruana, o mediante su pasaporte o carné de extranjería para personas de nacionalidad extranjera.
La información proporcionada por los solicitantes de nacionalidad peruana será validada por la ER de SOFTNET a través de un mecanismo de consulta a las bases de datos del RENIEC, incluyendo el uso de identificación biométrica mediante huella dactilar (servicio AFIS de RENIEC).
En el caso de solicitantes de nacionalidad extranjera, se acreditará su existencia y vigencia mediante su pasaporte o carné de extranjería.
De manera general, no se incluirá en los certificados, información no verificada del suscriptor. La IOFE permite una excepción en el caso de la dirección de correo electrónico del suscriptor. En este caso se comprobará que la dirección de correo electrónico que se incluye en el certificado es la que efectivamente desea incluir el solicitante. La ER de SOFTNET no asumirá la responsabilidad de

comprobar la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento, siendo todo esto responsabilidad del solicitante.

13.2. SOLICITUD DE CERTIFICADOS DE PERSONA JURÍDICA

13.2.1. Servicios brindados

La ER de SOFTNET brinda los siguientes servicios a personas jurídicas:

a) Atención de solicitudes de emisión de certificados para el representante legal, o certificado de atributo o de pertenencia a empresa, para personas jurídicas de nacionalidad peruana.
b) Atención de solicitudes de emisión de certificados para el representante legal, o certificado de atributo o de pertenencia a empresa, para personas jurídicas de nacionalidad extranjera.
c) Atención de solicitudes de emisión de certificados para agentes automatizados o certificado de TSA/TSU, para personas jurídicas de nacionalidad peruana, como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.
d) Atención de solicitudes de emisión de certificados para agentes automatizados o certificado de TSA/TSU, para personas jurídicas de nacionalidad extranjera, como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

13.2.2. Autorizados para realizar la solicitud

La solicitud debe ser hecha por un representante designado por la persona jurídica, el cual deberá presentar un documento que acredite dichas facultades de representación.

13.2.3. Modalidades de atención

La solicitud puede ser realizada mediante un contrato de Prestación de Servicio de Certificación Digital para la emisión de certificados digitales, el cual puede ser celebrado de alguna de las siguientes formas:

- De manera presencial en las instalaciones de SOFTNET en calidad de ER de la EC asociada.
- De manera presencial en las instalaciones del cliente, o un lugar designado por éste en presencia de un representante de la ER.
- Cuando la persona jurídica se encuentre en provincia, la persona autorizada puede acudir a un notario que certifique la firma del contrato y la identidad del firmante. El contrato deberá ser enviado a las oficinas de SOFTNET.
- Si la persona autorizada ya ha sido identificada y sus poderes de representación aún se encuentran vigentes, puede enviar el documento firmado de manera manuscrita (certificada mediante notario) o de manera digital a SOFTNET. Si sus poderes no se encuentran vigentes, debe adjuntar además un nuevo documento de representación.
- De manera virtual, previa verificación de los documentos solicitados ante los entes rectores (RENIEC, Migraciones, otros), se realizara a través de la plataforma de Microsoft que se encuentra debidamente licenciada y que cuenta con los medios de seguridad establecidos por Microsoft a sus servicios, permitirá que a través de una videoconferencia el Operador asignado guie en el proceso de verificación de identidad y de emisión del certificado a través de la plataforma de generación de certificados digitales.

13.2.4. Solicitud de certificado para persona jurídica

En el caso de certificados de representante legal o de certificados de atributos o de pertenencia a empresa, la persona jurídica se considera como aspirante a titular del certificado y los empleados vienen a ser los aspirantes a suscriptor.
El solicitante deberá especificar en su solicitud la lista de suscriptores y el tipo de atributo al que corresponderá cada certificado. Esta lista deberá ser debidamente firmada por la persona autorizada y se adicionará al contrato como adenda a éste en cada nueva oportunidad que se requieran certificados para nuevos suscriptores.

13.2.5. Periodo de vigencia de los certificados

En el caso de los certificados de representante legal o de certificado de atributos o de pertenencia a empresa, el periodo de vigencia del certificado solicitado no deberá exceder el periodo de tres (3) años de acuerdo a la legislación vigente.
En el caso de certificados para agentes automatizados o para TSA/TSU, el periodo de vigencia puede variar de acuerdo a lo establecido en la PC de la EC asociada.

13.2.6. Reconocimiento, autenticación y rol de las marcas registradas

Los solicitantes de certificados de personas jurídicas no deben incluir nombres en las solicitudes que puedan suponer infracción de derechos de terceros. La ER de SOFTNET tiene el derecho de rechazar una solicitud de certificado a causa de conflicto de nombres, puesto que no se podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente.
Mediante la verificación de la documentación e información presentada por el solicitante contra los Registros Públicos o la embajada correspondiente, SOFTNET en calidad de ER de una EC asociada determinará la validez del nombre de la persona jurídica. Sin embargo, no le corresponde a SOFTNET determinar si un solicitante de certificados le asiste algún tipo de derecho sobre el nombre que aparece en una solicitud de certificado, asimismo, no le corresponde resolver ninguna disputa concerniente a la propiedad de nombres de personas naturales o jurídicas, nombres de dominio, marcas o nombres comerciales.

13.2.7. Identificación y autenticación de solicitantes de certificados de persona jurídica

El solicitante deberá acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva con el documento de vigencia respectivo expedido por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente. La información proporcionada por los solicitantes será validada a través de la consulta a la Superintendencia Nacional de los Registros Públicos.
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 expedido por la autoridad competente en su país de origen.

13.2.8. Contrato del titular

La persona autorizada, debidamente acreditada, deberá firmar el contrato, que en adelante llamaremos "contrato del titular". A través de dicho contrato, el titular deberá declarar tener conocimiento de los términos y condiciones aplicables a los certificados.
La celebración de dicho contrato deberá realizarse antes de la emisión de los certificados.

13.2.9. Verificación de suscriptores

Los aspirantes a suscriptores deben ser validados en cualquiera de las siguientes modalidades:

- De manera presencial en las instalaciones de SOFTNET en calidad de ER de la EC asociada.
- De manera presencial en las instalaciones del cliente, o un lugar designado por éste en presencia de un representante de la ER.
- Cuando el suscriptor se encuentre en provincia y es otro distinto a la persona autorizada que firma el contrato del titular, puede acudir a un notario que certifique su identidad y manifestación de voluntad de requerir un certificado de representante legal o un certificado de atributo o de pertenencia a empresa. Dicho documento notarial deberá ser enviado a las oficinas de SOFTNET.

Cuando un individuo solicite la emisión de un certificado que sirva para acreditar el ejercicio de un cargo en concreto, la ER debe requerir a este solicitante las pruebas que evidencien su cargo, incluyendo la facultad de actuar en nombre de la persona jurídica en la que ocupa dicho cargo.

13.2.10. Identificación y autenticación de suscriptor

El aspirante a suscriptor debe presentarse en persona ante un funcionario de la ER de SOFTNET portando el original de su documento de identidad, esto es, DNI vigente para personas de nacionalidad peruana, o mediante su pasaporte o carné de extranjería para personas de nacionalidad extranjera.
La información proporcionada por los solicitantes de nacionalidad peruana será validada por la ER de SOFTNET a través de un mecanismo de consulta a las bases de datos del RENIEC, incluyendo el uso de identificación biométrica mediante huella dactilar (servicio AFIS de RENIEC).
En el caso de solicitantes de nacionalidad extranjera, se acreditará su existencia y vigencia mediante su pasaporte o carnet de extranjería.
De manera general, no se incluirá en los certificados, información no verificada del suscriptor o el titular según sea el caso. La IOFE permite una excepción en el caso de la dirección de correo electrónico del suscriptor. En este caso se comprobará que la dirección de correo electrónico que se incluye en el certificado es la que efectivamente desea incluir el solicitante. La ER de SOFTNET no asumirá la responsabilidad de comprobar la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento, siendo todo esto responsabilidad del solicitante.

13.3. USO Y ALMACENAMIENTO DEL CERTIFICADO DIGITAL

13.3.1. Certificados para Sistemas o Dispositivos

En el caso que el certificado esté destinado para ser usado por un agente automatizado, o en un dispositivo criptográfico centralizado (HSM) o una TSA/TSU, la solicitud debe ser hecha por la persona

responsable o autorizada para el uso del Certificado Digital. En este caso, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona natural o jurídica. La atribución de responsabilidad, para tales efectos corresponde al titular o representante legal.

El solicitante deberá especificar en su solicitud el propósito del certificado y el módulo criptográfico a emplear. Esta solicitud deberá ser debidamente firmada por el titular o la persona autorizada y se adicionará al contrato como adenda a éste en cada nueva oportunidad que se requieran nuevos certificados.

14. PROCESAMIENTO DE LA SOLICITUD DE EMISIÓN DE CERTIFICADO

14.1. RECHAZO DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO

La solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE, esto es, al no acreditarse:

a) Tratándose de personas naturales (suscriptor), el tener plena capacidad de ejercicio de sus derechos civiles.
b) Tratándose de personas jurídicas (titular), la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con una persona autorizada debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.
Una EC puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por SOFTNET en calidad de ER de la EC asociada.

14.2. APROBACIÓN DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO

En caso de que una solicitud sea aprobada por SOFTNET en calidad de ER de una EC asociada se realizará lo siguiente:

a) Comunicar a la EC asociada su aprobación para la emisión del certificado mediante un sistema web con control de acceso y la protección de un canal SSL. Este sistema es brindado, administrado y protegido por la EC asociada.
b) Se requerirá la firma del acta de conformidad de entrega de certificado digital por parte del suscriptor.

14.3. REGISTRO DE DOCUMENTOS

SOFTNET registrará y archivará la solicitud, los contratos firmados y los documentos de sustento presentados por el solicitante. Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad de la ER.

14.4. MÉTODO PARA PROBAR LA POSESIÓN DE LA CLAVE PRIVADA

La generación del par de claves debe realizarse bajo presencia y responsabilidad no transferible del suscriptor, en presencia del Operador de Registro o del Asistente de Validación de Identidad de SOFTNET en calidad de ER de la EC asociada (conforme a lo estipulado en la CP de ésta), en un módulo criptográfico con la certificación FIPS 140-2. Sin embargo, solamente el suscriptor deberá conocer las claves de acceso al módulo criptográfico donde se realiza la generación de la clave.
Luego, se realizará la petición segura del certificado a la EC asociada en formato PKCS#10, realizando con ello la prueba de la posesión de la clave privada.

14.5. TIEMPO PARA EL PROCESAMIENTO DE LA SOLICITUD DE UN CERTIFICADO

Una vez validada la información proporcionada por el suscriptor, si el resultado de la validación es positivo, SOFTNET en calidad de ER de la EC asociada enviará a ésta la autorización de la emisión del certificado de manera inmediata.
El máximo tiempo de respuesta para la emisión del certificado será de 05 días, luego de haber sido aprobada la validación de identidad y del pago respectivo.

14.6. EMISIÓN DEL CERTIFICADO

La emisión del certificado será realizada por la EC asociada. El certificado será entregado de acuerdo a lo indicado en la DPC de la EC asociada. En lo posible se enviará un mensaje con las instrucciones de entrega del certificado a la dirección de correo electrónico del suscriptor, registrado en su solicitud.

15. SOLICITUD DE REVOCACIÓN DE CERTIFICADO

15.1. CIRCUNSTANCIAS PARA REALIZAR LA SOLICITUD

El titular y el suscriptor del certificado están obligados, bajo responsabilidad, a solicitar la revocación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias:

- Por exposición, puesta en peligro o uso indebido de la clave privada.
- Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.
- Revocación de las facultades de representación y/o poderes de los representantes legales o apoderados de la persona jurídica
- Cuando la información contenida en el certificado ya no resulte correcta.
- Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la EC asociada.
- Cuando el suscriptor o titular incumple las obligaciones a las que se encuentra comprometido dentro de la IOFE a través de lo estipulado en el contrato del suscriptor y/o titular.
- Por mandato de un juez.

15.2. SOLICITUD DE REVOCACIÓN DE CERTIFICADO

15.2.1. Servicios brindados

SOFTNET brinda los siguientes servicios asociados a la cancelación o revocación de un certificado:

a) Atención de solicitudes realizadas por una persona natural (el suscriptor del certificado).
b) Atención de solicitudes realizadas por una persona jurídica (el titular del certificado) a través de la persona autorizada u otra que acredite los poderes necesarios para realizar dicha solicitud.
c) Atención de solicitudes de terceros que acrediten una razón válida para requerir la revocación de un certificado.

15.2.2. Autorizados para realizar la solicitud

De acuerdo a lo estipulado por la Ley de Firmas y Certificados Digitales y su Reglamento, las personas que pueden solicitar la revocación de un certificado son:

- El titular del certificado
- El suscriptor del certificado.
- La EC o ER que emitió el certificado.
- Un juez que de acuerdo a ley emita un mandato judicial para revocar el certificado.
- Un tercero que tenga pruebas fehacientes del uso indebido del certificado, el compromiso de clave u otro motivo de revocación mencionado en la ley o en su reglamento, en las guías de acreditación o en el presente documento.

15.2.3. Modalidades de atención

- De manera presencial en las instalaciones de SOFTNET en calidad de la ER de la EC asociada.
- De manera presencial en las instalaciones del cliente, o un lugar designado por éste en presencia de un representante de la ER.
- De manera remota, mediante un documento o correo electrónico firmado digitalmente por el representante asignado por la persona jurídica o por el suscriptor. El certificado digital a emplear no debe ser el que se desea revocar.
- De manera remota en una comunicación directa con la EC asociada, según los medios descritos en su DPC, esto puede ser mediante un control de acceso o contraseña brindados al suscriptor en el momento de la solicitud de emisión del certificados.
- Para todos los demás actores, diferentes a los suscriptores y titulares, la solicitud deberá ser de manera presencial en las instalaciones de SOFTNET en calidad de ER de la EC asociada.

La EC no requerirá realizar la solicitud a la ER en los casos que el suscriptor haya infringido las obligaciones descritas en su contrato o en caso sea necesario por revocación del certificado de la EC asociada.

La EC asociada puede revocar los certificados que ha emitido, siempre y cuando los motivos de revocación estén claramente especificados en su CPS y se encuentren de acuerdo con la legislación vigente.

15.2.4. Identificación y autenticación de los solicitantes

En los casos de que la solicitud sea presencial:

- El suscriptor debe presentarse en las oficinas de la ER portando su documento de identidad, esto es, DNI vigente para personas de nacionalidad peruana, o mediante su pasaporte o carné de extranjería para personas de nacionalidad extranjera.
- El representante asignado por la persona jurídica debe presentarse en las oficinas de la ER portando su documento de identidad, documentos que acrediten dicha representación y la voluntad de dicha persona jurídica.
- Un tercero (diferentes a la EC asociada, al suscriptor o al titular) deberá presentarse en las oficinas de la ER portando su documento de identidad y las pruebas fehacientes del uso indebido del certificado, el compromiso de la clave u otro motivo de revocación de acuerdo a la ley vigente, junto a la orden judicial respectiva.

15.2.5. Solicitud de revocación de certificado

Cuando la solicitud es presentada a la ER de SOFTNET, el solicitante debera especificar en su solicitud, la lista de suscriptores y el número de serie de su certificado. También se deberá indicar la razón por la que se solicita dicha revocación. Esta lista deberá ser debidamente firmada por una persona autorizada para realizar la solicitud tal como se indica en este documento

16. PROCESAMIENTO DE LA SOLICITUD DE REVOCACIÓN

16.1. RECHAZO DE LA SOLICITUD DE REVOCACIÓN DE UN CERTIFICADO

La solicitud de revocación de certificado será rechazada en caso no se cumpla con alguna de las modalidades de solicitud o que el solicitante no se encuentre debidamente autorizado conforme a lo descrito en el presente documento.
La solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE, esto es, al no acreditarse:

a) Tratándose de personas naturales (suscriptor), el tener plena capacidad de ejercicio de sus derechos civiles.
b) Tratándose de personas jurídicas (titular), la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con una persona autorizada debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

Una EC puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por SOFTNET en calidad de ER de la EC asociada.

16.2. APROBACIÓN DE LA SOLICITUD DE REVOCACIÓN DE UN CERTIFICADO

En caso de que una solicitud sea aprobada por SOFTNET en calidad de ER de la EC asociada realizará lo siguiente:

a) Comunicar a la EC asociada su aprobación para la revocación del certificado mediante un sistema web con control de acceso y la protección de un canal SSL. Este sistema será brindado, administrado y protegido por la EC asociada.
b) Una copia de dicha solicitud firmada será enviada a la EC asociada o almacenada en SOFTNET en calidad de ER de la EC asociada conforme a los acuerdos celebrados con dicha EC.

16.3. REGISTRO DE DOCUMENTOS

La ER de SOFTNET registrará y archivará la solicitud y los documentos de sustento presentados por el solicitante dejando constancia de la persona que efectúa la solicitud, la relación que tiene ésta con el titular, las razones de la solicitud, las acciones tomadas para la verificación de la veracidad de la solicitud, fecha y hora de la revocación y de la notificación de la misma a la EC asociada, sus suscriptores y los terceros que confían.
Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.
En caso que no se acepte la revocación, se dejará constancia de los hechos que motivaron dicha denegatoria.

16.4. TIEMPO PARA EL PROCESAMIENTO DE LA SOLICITUD DE REVOCACIÓN

Una vez validada la información proporcionada por el suscriptor, si el resultado de la validación es positivo, SOFTNET en calidad de ER enviará a la EC asociada la autorización de la revocación del certificado de manera inmediata.
El máximo tiempo de respuesta para la revocación del certificado dependerá de lo establecido en la CP y CPS de la EC asociada.

17. REVOCACIÓN DEL CERTIFICADO

La revocación del certificado será comunicada al suscriptor y titular mediante el correo electrónico del suscriptor, registrado en su solicitud.

18. GESTIÓN DE OPERACIONES

18.1. MÓDULO CRIPTOGRÁFICO

La generación de claves de los suscriptores debe ser realizada en módulos criptográficos FIPS 140-2.
Los módulos criptográficos usados por los Operadores de Registro deben cumplir los requerimientos o ser equivalentes a los requerimientos de FIPS 140-2 nivel de seguridad 2 como mínimo.

18.2. RESTRICCIONES DE LA GENERACIÓN DE CLAVES

Las claves pueden ser generadas solamente por los propios suscriptores.

18.3. DEPÓSITO DE CLAVE PRIVADA

SoftNet, como ER, no genera copias de las claves privadas de los suscriptores ni de los Operadores de Registro en ninguna modalidad.

18.4. DATOS DE ACTIVACIÓN

Los datos de activación del módulo criptográfico serán administrados por los suscriptores. En caso de obtener módulos criptográficos de SoftNet, se brindará la información correspondiente a los suscriptores para que puedan realizar la activación de su dispositivo.

19. CONTROLES DE SEGURIDAD COMPUTACIONAL

Los sistemas de registro utilizados por SoftNet son provistos y administrados por la EC asociada. La ER sólo accede a estos sistemas vía web con acceso vía certificados digitales de los Operadores de Registro.
Respecto a la seguridad de la información se sigue el esquema ISO 27001.

19.1. REQUISITOS TÉCNICOS DE SEGURIDAD ESPECÍFICOS

LaEC asociada cuenta con una infraestructura tecnológica debidamente monitoreada y equipada con elementos de seguridad requeridos para garantizar una alta disponibilidad y confianza en los servicios ofrecidos a sus titulares y terceros de confianza.
La información relacionada con Seguridad de la Información es considerada como confidencial y por tanto solo puede ser suministrada a aquellos entes acreditados que requieran de su conocimiento.

19.2. EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

El sistema de gestión de la seguridad de la Información evalúa los procesos relacionados con la infraestructura tecnológica con el fin de identificar posibles debilidades y definir los planes de mejoramiento continuo con el apoyo de las auditorias permanentes y periódicas.

20. AUDITORÍAS DE COMPATIBILIDAD Y OTRAS EVALUACIONES

De acuerdo con los lineamientos establecidos por la AAC, se llevarán a cabo auditorías externas anuales que tendrán como objetivo evaluar la conformidad de las operaciones y que éstas se encuentren alineadas al marco de la IOFE. Sin perjuicio de las auditorías eternas, se realizarán auditorías internas o evaluaciones de conformidad de la ER de SoftNet, a fin de verificar el cumplimiento de los procedimientos establecidos y velar por la seguridad de la información.

20.1. FRECUENCIA Y CIRCUNSTANCIA DE LA EVALUACIÓN

La ER de SoftNet llevará a cabo una auditoría externa anual que evalúe la conformidad de las operaciones y que estas e encuentran alineadas al marco de la IOFE. Esta auditoría también podrá comprender la evaluación de cumplimiento de lo establecido en el presente documento.
Sin perjuicio de las auditorías externas, se realizarán auditorías internas o evaluaciones de conformidad de la ER de SoftNet en cualquier momento, a causa de alguna sospecha de incumplimiento de alguna medida de seguridad o de los procedimientos establecidos por ésta. Dicha auditoría puede comprender la evaluación del cumplimiento del Plan de Privacidad, Política de Seguridad de la Información y demás documentos normativos.
Las evaluaciones técnicas del INDECOPI se llevarán llevarse a cabo una vez al año y cada vez que el INDECOPI lo requiera.
El resultado de las auditorías será informado al Responsable de la ER de SoftNet de tal forma que se coordine el desarrollo de acciones correctivas, de ser el caso, para el levantamiento de no conformidades o el mejoramiento de procedimientos.

20.2. CALIFICACIONES DE LOS AUDITORES

La ejecución de un procedimiento de auditoría externa se llevará a cabo por auditores independientes de SoftNet. El perfil profesional de estos auditores incluye experiencia en tecnologías PKI, en seguridad y tecnologías de la información y procesos de auditoría.
Para el caso de las auditorias de seguimiento anual para el mantenimiento de la acreditación, la AAC proporcionará un listado de profesionales aptos que puedan realizar dicho procedimiento.

20.3. RELACIÓN DEL AUDITOR CON LA ER

Los auditores o asesores deben ser independientes de SoftNet. En el caso de los auditores internos, SoftNet deberá definir los requisitos y cualificaciones del auditor teniendo cuidado en que no tenga relación funcional con el área objeto de la auditoría.

20.4. ELEMENTOS CUBIERTOS POR LA EVALUACIÓN

El auditor evaluará el cumplimiento de la implementación de las prácticas del personal, procedimientos y medidas técnicas desplegadas por la ER de SoftNet dentro del marco de la IOFE.
En tal sentido, los principales aspectos cubiertos por la auditoría son los que se detallan a continuación:

- Identificación y autenticación
- Servicios y funciones operacionales
- Controles de seguridad física
- Controles para la ejecución de los procedimientos
- Controles de seguridad técnicos

20.5. ACCIONES A SER TOMADAS FRENTE A RESULTADOS DEFICIENTES

La identificación de deficiencias detectadas como resultado de una auditoría externa dará lugar a la implementación de medidas correctivas. De corresponder a un procedimiento de auditoría de

seguimiento anual, la AAC determinará las acciones que deberán ser adoptada por parte de la ER de SoftNet.

20.6. PUBLICACIÓN DE RESULTADOS

El auditor externo para un procedimiento de auditoría de seguimiento anual, comunicará el resultado de dicha auditoría a la AAC y a la ER de SoftNet, el cual podrá ser publicado por INDECOPI.

21. OTRAS MATERIAS DE NEGOCIO Y LEGALES

21.1. TARIFAS

Las tarifas por los servicios de registro y certificación digital serán puestas a disposición de los usuarios en las cotizaciones remitidas a solicitud de estos.

21.2. POLÍTICAS DE REEMBOLSO

No se aplican reembolsos, sin embargo, de ser requeridos, los detalles sobre la política de reembolso por los servicios de registro serán definidos en los respectivos contratos.

21.3. RESPONSABILIDAD FINANCIERA

21.3.1. Cobertura de seguro

SOFTNET cuenta con un seguro de responsabilidad civil según los requerimientos establecidos para los PSC por la AAC en la Guía de Acreditación respectiva. El referido seguro podrá cubrir el riesgo de la responsabilidad por los daños y perjuicios que se pudiese ocasionar a terceros como resultado de las actividades a cargo de la ER de SOFTNET, hasta por un monto de US $ 30,000 dólares americanos.

21.3.2. Otros activos

SOFTNET es una empresa solvente que cuenta con infraestructura e instalaciones necesarias para brindar los servicios de una ER.

21.3.3. Cobertura de seguro o garantía para entidades finales

SOFTNET como ER no otorga seguro o garantía para entidades finales.

21.4. CONFIDENCIALIDAD DE LA INFORMACIÓN DE NEGOCIO

La ER de SOFTNET mantendrá la confidencialidad de toda aquella información que ha sido clasificada como “confidencial”.

21.4.1. Alcance de la información confidencial

La ER de SOFTNET declara expresamente como información confidencial, la misma que no podrá ser divulgada a terceros y que se mantendrá con carácter de reservado, excepto en aquellos supuestamente previsto legalmente, la siguiente:

- Material o información reservada de le ER de SOFTNET incluyendo contrato, planes de negocio e información relacionada con derechos de propiedad intelectual.
- La información de la ER proporcionada por la EC asociada o, en caso corresponda, por proveedores y otras personas con las que la ER tiene el deber de guardar secreto establecido de modo convencional.
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los titulares y suscriptores.
- Información que pueda permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los titulares, suscriptores y el tercero que confía.
- La razón que motivó la revocación de un certificado digital.
- Información personal provista por los titulares y suscriptores que sea la autorizada para estar contenida en los certificados digitales y en la CRL.
- Toda información clasificada como confidencial.
- Las indicadas en la Política de Seguridad.

21.4.2. Información no contenida en el rubro de información confidencial

Se considera información pública y por tanto accesible por terceros:

- La contenida en la presente DPR.
- La contenida en la Política de Privacidad.
- Los certificados digitales emitidos por la EC asociada previa autorización de la ER de SOFTNET, así como la información contenida en éstos y el estado de los mismos.
- La CRL.
- Otra información clasificada como pública.

En todo caso, el acceso a dicha información será permitido sin perjuicio que la ER aplique controles de seguridad pertinentes con el fin de proteger la autenticidad e integridad de los documentos, así como impedir que personas no autorizadas puedan añadir, modificar o suprimir contenido.

21.4.3. Responsabilidad de protección de la información confidencial

El personal de la ER, así como el personal de algún proveedor que participen en cualquiera de las actividades del proceso a cargo de aquella están obligados a guardar secreto sobre la información clasificada como “confidencial”, según lo señalado en el Plan de Privacidad.

21.5. PRIVACIDAD DE LA INFORMACIÓN PERSONAL

De conformidad con lo establecido en la Ley N° 29733 – Ley de Protección de Datos Personales, se considera como datos personales, toda información sobre una persona natural que la identifica o la hace identificable a través de medios que puedan ser razonablemente utilizados.

La ER asegura a los titulares y suscriptores el adecuado tratamiento de sus datos personales, los cuales serán tratados para los fines propios de la prestación del servicio de certificación digital o para otros propósitos relacionados con dicho servicio, y que permitan otorgar confianza al tercero que confía o tercer usuario, pudiendo ellos verificar el estado del certificado digital emitido por la EC asociada.

21.5.1. Plan de privacidad

El Plan de Privacidad de la ER de SOFTNET recoge los principios de la Ley antes indicada, así como la Norma Marco de Privacidad del APEC, aprobada mediante resolución N° 030-2008-RT-INDECOPI.
El referido Plan de Privacidad establece, entre otros, las directrices que deben cumplir el personal de la ER y terceros que presten sus servicios como contratistas, así como las directrices respecto de la recolección de datos personales, uso y tratamientos de estos, transferencia de la información, mecanismos de acceso a la información personal y las medidas de seguridad destinadas a garantizar la integridad y confidencialidad de la información.
El Plan de Privacidad es catalogado como información confidencial y sólo se proporciona al personal de la ER, de la EC asociada, y a quien acredite la necesidad de conocerlo, como en el caso de las auditorías externas o internas.
Las sanciones que la ER aplicará al personal involucrado en la prestación del servicio de certificación digital son los establecidas por SOFTNET.

21.5.2. Información tratada como privada

La ER declara expresamente como información personal de carácter privado, a toda aquella información que no se encuentre contenida en los certificados digitales ni en la CRL.
En todo caso, la información siguiente es considerada como privada:

- Solicitudes de certificados digitales, aprobadas o denegadas, así como toda otra información personal que tenga carácter privado y ha sido obtenida para la expedición y mantenimiento del certificado digital.
- Toda la documentación contenida en el expediente que custodia la ER y que no tome parte de la información contenida en el certificado digital.
- La causal que originó la revocación del certificado digital.
- Toda información personal que tenga el carácter de “información privada”.

La información personal considerada como privada de acuerdo con el Plan de Privacidad de la ER es protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizada.

21.5.3. Información no considerada como privada

La información personal no considerada privada es aquella que se incluye en los certificados digitales y en la CRL. Se detalla, pero no limita a:

- Certificados emitidos o en trámite de emisión.
- Datos de identificación que figuran en el certificado digital del titular y suscriptor y que sirven para autenticar a aquel.
- Usos y límites de uso de los certificados digitales.

Por consiguiente, la información que se hará pública es la siguiente:

a) Certificados digitales emitidos o en trámite de emisión.
b) Certificados digitales cancelados.
c) Datos de identificación que figuran en el certificado digital del titular y suscriptor.

d) Usos y límites de uso de los certificados digitales.
e) Aquella información personal que los titulares y suscriptores soliciten o autoricen que se publique.
f) El periodo de validez del certificado digital, así como la fecha de emisión y fecha de caducidad del certificado digital.
g) El número de serie del certificado digital.

21.5.4. Responsabilidad de protección de la información privada

La ER de SOFTNET cumple con los principios y las disposiciones establecidas en la Ley N° 29733 – Ley de Protección de Datos Personales. En tal sentido, ha implementado medidas de seguridad de índole organizativas y técnicas orientadas a mantener la más estricta confidencialidad de la información y de los datos personales de carácter privado de los titulares y suscriptores de los certificados digitales, recogida dentro del marco de la prestación del servicio de certificación digital.

21.5.5. Notificación y consentimiento para el uso de información

En los diferentes formatos empleados se especifican los datos personales de los titulares y suscriptores que son recolectados por la ER o directamente a través de la plataforma de la EC asociada.
De conformidad con lo dispuesto en el numeral 1 del Artículo 14 de la Ley N° 29733 – Ley de Protección de Datos Personales, la ER está exceptuada de solicitar consentimiento al titular de los datos, para el tratamiento y transferencia de sus datos personales.
No obstante, la ER mediante la Política de Privacidad informa al titular y suscriptor respecto de:

- Los datos personales que recolecta.
- Fines del uso y tratamiento de la información personal.
- La información personal pública y de carácter privado.
- Las medidas de seguridad para proteger la información personal de carácter privado.
- Las circunstancias bajo las cuales la información personal será divulgada o transferida.
- Los derechos del titular y suscriptor, entre otros.

21.5.6. Divulgación realizada con motivo de un proceso judicial o administrativo

Excepcionalmente, los datos personales de carácter privado o la información confidencial del titular y suscriptor serán revelados o comunicados al Poder Judicial cuando una orden judicial así lo exija o cuando ésta sea autorizada, de manera expresa, por el titular y suscriptor.

21.6. DERECHOS DE PROPIEDAD INTELECTUAL

Todos los derechos de propiedad intelectual respecto a la plataforma de registro son propiedad de la EC asociada (por ejemplo de eMudhra, como PSC de SOFTNET) y de uso exclusivo de sus entidades de registro asociadas, entre ellas la ER de SOFTNET.
Las claves privadas y las claves públicas son propiedad del titular del certificado asociado.

21.7. RESPONSABILIDADES Y GARANTÍAS

21.7.1. Responsabilidades y garantías de la EC

No aplica a la ER de SOFTNET.

21.7.2. Responsabilidades y garantías de la ER

Son obligaciones de la ER:

- Realizar sus operaciones de conformidad con esta DPR.
- Comprobar exhaustivamente la identidad de los solicitantes.
- Gestionar, a través de la plataforma de la EC asociada, la generación de los certificados digitales.
- Gestionar, a través de la plataforma de la EC asociada, la revocación de los certificados digitales cuando estos procedimientos sean solicitados a la ER.
- Mantener la confidencialidad de la información personal que tenga carácter privado de los titulares y suscriptores de certificados digitales, limitando su empleo a las necesidades propias del servicio de certificación digital, salvo orden judicial o pedido del titular y suscriptor del certificado digital.

La ER asume que la información personal proporcionada por los titulares y suscriptores es verídica. Estos son responsables de comunicar, de manera inmediata a la ER, cualquier modificación en los mismos- Los titulares y suscriptores asumirán las responsabilidades por los daños y perjuicios que pudiera causar por proporcionar datos falsos, incompletos o inexactos. En ese sentido, la ER está exenta de toda responsabilidad cuando el error o la omisión de algún dato contenido en el certificado digital deviene de la información consignada o validada por los titulares y suscriptores en las respectivas solicitudes de emisión y contratos.

Estas obligaciones se encuentran recogidas en los contratos de prestación de servicios de certificación digital suscrito por los titulares y suscriptores.

21.7.3. Responsabilidades y garantías de los titulares y suscriptores

Son obligaciones de los titulares y suscriptores del certificado digital:

- Entregar información veraz bajo su responsabilidad.
- Actualizar la información proporcionada a la ER cuando éstos ya no resulten exactos o sean incorrectos.
- Custodiar su contraseña o clave de identificación personal de acceso a su clave privada de forma diligente, tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizado.
- Observar las condiciones establecidas por la EC asociada para la utilización del certificado digital y la generación de firmas digitales.
- Realizar un uso indebido y correcto del certificado digital.
- Notificar de inmediato a la ER en caso de que detecte que se ha incluido información incorrecta o inexacta en el certificado digital.
- Solicitar inmediatamente a la ER, o directamente a la EC asociada, la revocación de su certificado digital en caso de tener conocimiento o sospecha de la ocurrencia de alguna de las siguientes circunstancias.

a) Exposición, puesta en peligro o uso indebido de la clave privada o de la contraseña o PIN de acceso a su clave privada.
b) Deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada o la contraseña o PIN de acceso a su clave privada.

El compromiso de la clave privada del certificado digital entre otras causas puede ser por pérdida, robo, conocimiento de un tercero de la clave personal de acceso.

- Solicitar inmediatamente a la ER, o directamente a la EC asociada, la revocación de su certificado digital cuando:
  a) La información contenida en el certificado digital ya no resulte correcta.
  b) El titular y suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la EC asociada.

Estas obligaciones se encuentran recogidas en el respectivo contrato suscrito por titulares y suscriptores.

Asimismo, el titular y suscriptor del certificado asumirán las responsabilidades a que hubiere lugar por los daños y perjuicios que pudiese causar por proporcionar datos falsos, incompletos o inexactos. Así también es de su exclusiva responsabilidad el uso indebido, incorrecto o no acorde a los fines para el que fue emitido el certificado. A tales efectos, la ER de SOFTNET está excluida de toda responsabilidad.

21.7.4. Responsabilidades y garantías de los terceros que confían

Es obligación de los terceros que confían en los certificados emitidos por la EC asociada a través de la ER de SOFTNET:

- Verificar la validez de los certificados digitales en el momento de realizar cualquier transacción basada en los mismo mediante la comprobación que el certificado y su cadena de confianza son válidos, esto es, que no han caducado ni han sido revocados.
- No usar los certificados digitales fuera de los términos establecidos en el marco de la IOFE:
- Limitar la fiabilidad de los certificados digitales a los usos permitidos de los mismos.
- Dar lectura al presente documento.
- Tener pleno conocimiento de las garantías y responsabilidades aplicables en la aceptación y uso de los certificados digitales en los que confía y aceptar sujetarse a las mismas.

21.7.5. Responsabilidades y garantías de otros participantes

No intervienen otros participantes que los indicados.

21.8. EXENCIÓN DE GARANTÍAS

La ER de SOFTNET está exenta del pago de indemnización alguna en caso el hecho o circunstancia acaecida no sea consecuencia de lo declarado en la subsección 21.10.

21.9. LIMITACIONES A LA RESPONSABILIDAD

La ER de SOFTNET asume toda la responsabilidad sobre la correcta identificación de los titulares y suscriptores de los certificados digitales y la validación de sus datos, no obstante, la ER de SOFTNET está

exenta de responsabilidad alguna, en los casos que la AAC no considere responsabilidad de las ER acreditadas, como los que se detallan a continuación:

- Por daños derivados de o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo del titular y suscriptor
- Cuando el error o la omisión de algún dato contenido en el certificado digital deviene de la información consignada por el titular y suscriptor en los respectivos formatos de solicitud de emisión.
- Por cualquier violación a la confidencialidad que en el uso de datos personales pudieran incurrir el propio titular o suscriptor del certificado digital.
- Cuando el titular o suscriptor no han tenido la debida diligencia o cuidado en la creación de su contraseña o PIN de acceso a su clave privada.

De igual modo, la ER no será responsable de:

- La utilización incorrecta de los certificados digitales ni de las claves, así como de cualquier daño indirecto que pueda resultar de la utilización del certificado o de la información almacenada en el dispositivo criptográfico que resguarda la clave privada.
- Los daños que puedan derivarse de aquellas operaciones en que se hayan incumplido las limitaciones de uso del certificado digital.
- El contenido de aquellos documentos firmados digitalmente por el titular o suscriptor.

21.10. INDEMNIZACIONES

La ER dispondrá de una garantía con cobertura suficiente de responsabilidad civil a través del seguro contratado por SOFTNET. El referido seguro cubrirá el riesgo de la responsabilidad por daños y perjuicios que se pudiese ocasionar a terceros como resultado de las actividades a cargo de la ER.

21.11. TÉRMINO Y TERMINACIÓN

21.11.1. Término

La presente DPR entra en vigor desde el momento que es aprobada por la AAC, dentro del procedimiento administrativo de acreditación de la ER de SOFTNET, que implica su ingreso a la IOFE, manteniendo su validez durante un periodo máximo de cinco (5) años, de acuerdo con la legislación vigente. No obstante, dicho documento podrá ser modificado cada vez que lo determine la ER o la AAC.

En el supuesto que caducase la acreditación o de un cese de operaciones de la ER, toda la documentación relativa queda sin vigencia, aplicándose en tal situación lo señalado en la subsección 21.11.2.

21.11.2. Terminación

En caso cese de las actividades de la ER, SOFTNET informará a la AAC con sesenta (60) días de anticipación y a los titulares y suscriptores con treinta (30) días de anticipación.

21.11.3. Efecto de terminación y supervivencia

Las obligaciones y restricciones que establece esta DPR, en referencia a auditorías, información confidencial, obligaciones y responsabilidades, nacidas bajo la vigencia del presente documento, subsistirán tras su sustitución por una nueva versión en todo en lo que no se oponga a ésta.

21.12. NOTIFICACIONES Y COMUNICACIONES INDIVIDUALES CON LOS PARTICIPANTES

Sin perjuicio de lo señalado en la presente DPR, sobre requisitos operacionales del ciclo de vida de los certificados, los titulares y suscriptores podrán consultar en cualquier momento el periodo de validez de sus certificados digitales a través de la página web de la EC asociada.

21.13. ENMENDADURAS

21.13.1. Procedimiento para enmendaduras

De conformidad con la legislación vigente, la ER, en caso se modifique el contenido del presente documento, presentará a la AAC la nueva versión de la DPR para su respectiva aprobación.

21.13.2. Mecanismo y periodo de notificación

La ER pondrá a disposición de la comunidad de usuarios la nueva versión de la DPR, una vez que la misma haya sido aprobada por la AAC.
El mecanismo de comunicación se efectuará a través de la página web de SOFTNET, surtiendo los efectos de una notificación válidamente emitida.

21.14. PROCEDIMIENTO SOBRE RESOLUCIÓN DE DISPUTAS

En caso el reclamo esté directamente relacionado con el servicio de certificación digital brindado por la ER, el titular o suscriptor se deberá acercar a la oficina de SOFTNET para presentar el reclamo.
Dicho reclamo será resuelto por SOFTNET en primera instancia. De no estar conforme, podrá presentar un recurso de apelación ante la AAC, cuyo veredicto corresponderá a la última instancia existente.

21.15. LEY APLICABLE

El funcionamiento y operaciones de la ER, así como la presente DPR estarán sujetos a la normatividad que resulte aplicable y en especial a las disposiciones siguientes:

- Ley N° 27269 - Ley de Firmas y Certificados Digitales.
- Reglamento de la Ley de Firmas y Certificados aprobado mediante el DS N° 052-2008-PCM y sus modificatorias, el DS N° 105-2012-PCM y DS N° 026-2016-PCM.
- Guía de Acreditación de Entidades de Registro
- Ley N° 29733 - Ley de Protección de Datos Personales y su Reglamento.

Así como a las disposiciones que sobre la materia dicte la AAC en el marco de la IOFE.

21.16. CONFORMIDAD CON LA LEY APLICABLE

Es responsabilidad de la ER, en la prestación de sus servicios, velar por el cumplimiento de la legislación aplicable recogida en la subsección Ley aplicable del presente documento y que la misma haya sido recogida en los correspondientes contratos.

21.17. CLÁUSULAS MISCELÁNEAS

21.17.1. Acuerdo íntegro

Los titulares y suscriptores de certificados digitales, así como los terceros que confían, deben observar en su totalidad el contenido del presente documento, así como las actualizaciones que relacionen sobre el mismo, los cuales estarán disponibles en la página web de SOFTNET.

21.17.2. Subrogación

Las funciones, deberes y derechos asignados a SOFTNET, en su calidad de ER, no serán objeto de cesión de ningún tipo a terceros, así como ninguna tercera entidad podrá subrogarse en dicha posición jurídica, salvo por disposición legal que expresamente disponga lo contrato.

21.17.3. Divisibildad

No aplica.

21.17.4. Ejecución

No aplica.

21.17.5. Fuerza mayor

La ER en ningún caso será responsable por daños o perjuicios causados por:

- Catástrofes naturales
- Casos de guerra
- Actos de terrorismo o sabotaje
- Otros actos de fuerza mayor

Sin perjuicio de lo expuesto, la ER dentro de lo posible asegurará la continuidad del negocio y recuperación ante desastres.

21.17.6. Otras cláusulas

La ER adicionalmente a lo señalado en esta DPR, podrá incluir otras disposiciones relacionadas a las actividades y operaciones que realizará dentro del marco de la IOFE.

Disposición de flexibilización para la verificación de Identidad

- La verificación de identidad en el marco del estado de emergencia sanitaria por el COVID ha extendido la facilidad de realizar la verificación de identidad a través de medios virtuales:
  "La Comisión de Gestión de la Infraestructura Oficial de Firma Electrónica (IOFE) del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Indecopi) resolvió flexibilizar temporalmente los requisitos para aquellas personas que nunca han tenido un certificado digital y ahora necesitan adquirirlo.

Para ello, la Comisión ha comunicado directamente a las empresas acreditadas que la verificación de la identidad de un solicitante de certificado digital puede llevarse a cabo mediante medios alternativos a la comparecencia física, como por ejemplo la verificación a través de cualquiera de las plataformas que la Internet ofrece para comunicaciones con cámara de video en tiempo real.

Esta decisión se refiere tanto a los usuarios cuyo certificado digital había expirado como a aquellos que lo solicitan por primera vez.

El propósito de la Comisión es facilitar las comunicaciones a distancia con pleno efecto legal en el actual momento de emergencia sanitaria debido al coronavirus Covid-19, en el cual las verificaciones presenciales para esta clase de actividades han sido suspendidas por mandato de normas legales de superior jerarquía.

Culminada esta etapa extraordinaria, se llevarán a cabo acciones de fiscalización y se volverá a exigir los requisitos ordinarios de verificación".

22. Historial de Cambios

Generales			
Propietario del Documento	*Carlos Dextre*	**Clasificación**	*Privada*
Aprobado por:	*Carlos Dextre*	**Fecha aprobación inicial**	*15/08/2020*

Fecha	*Versión*	*Descripción*	*Autor*
01/08/2020	*1.0*	*Documento Inicial*	*Coordinador de la seguridad de la Informacion*
15/08/2020	*1.0*	*Aprobacion*	*Representante de la ER*
15/08/2020	*1.0*	*Revision de Documento*	*Gerente de Productos y Servicios*
20/09/2020	*1.0*	*Revision del Documento*	*Coordinador de Seguridad de la Informacion*
20/09/2020	*1.0*	*Revision*	*Gerente de Productos y Servicios*
20/09/2020	*1.0*	*Aprobado*	*Representante de la ER*
20/10/2021	*1.0*	*Revision del Documento*	*Coordinador de Seguridad de la Informacion*
20/10/2021	*1.0*	*Revision*	*Gerente de Productos y Servicios*
20/10/2021	*1.0*	*Aprobado*	*Representante de la ER*
24/10/2022	*1.0*	*Revision del Documento*	*Gerente del Sistema Integrado de Gestion*
24/10/2022	*1.0*	*Revision*	*Gerente de Productos y Servicios*
24/10/2022	*1.0*	*Aprobado*	*Representante de la ER*
14/11/2024	*1.0*	*Revision de Documento*	*Jefe de Productos Servicios e Infraestructura Tecnologica*
14/11/2024	*1.0*	*Aprobacion*	*Representante de lña EC y ER*
15/10/2025	*1.0*	*Revision de Cargos*	*CISO – GSIG - Resp. Seguridad*

Fecha	*Versión*	*Descripción*	*Autor*
15/10/2025	*1.0*	*Revision de Documento*	*Administrador de la ER - JPSIT*
15/10/2025	*1.0*	*Aprobacion*	*Representante de la ER*
28/10/2025	*1.1*	*Ajuste para el Uso y Almacenamiento del CD* *13.3.1 Certificados para Sistemas o Dispositivos*	*CISO – GSIG - Resp. Seguridad*
28/10/2025	*1.1*	*Revision de Documento*	*Administrador de la ER - JPSIT*
28/10/2025	*1.1*	*Aprobacion*	*Representante de la ER*
10/12/2025	*1.2*	Modalidades de atención en los puntos 13.1.3 y 13.2.3 respecto a la atención Virtual, añadido en base a la auditoria realizada a la ER en nov del 2025, modifica la versión de la Declaración de Practicas a la 1.2	*CISO – GSIG - Resp. Seguridad*
10/12/2025	*1.2*	*Revision de Documento*	*Administrador de la ER - JPSIT*
10/12/2025	*1.2*	*Aprobacion*	*Representante de la ER*

Elaborado por: Pedro Rivera P.	Revisado y Aprobado por: M. Jhoel Sanchez B.	Revisado y Aprobado por: Carlos Dextre P.
V°B°	V°B°	V°B°
Cargo: CISO – GSIG – Oficial de Cumplimiento	Cargo: *Jefe de Productos Servicios e Infraestructura Tecnológica*	Cargo: Gerente General Responsable de la ER