SOFTNET

PLAN DE PRIVACIDAD

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)

2. OBJETIVO

Este documento tiene como objetivo la descripción de operaciones y prácticas de protección de datos personales que utiliza emSign como Proveedor de Servicios de Certificación de SoftNet para la administración de sus servicios como Entidad de Certificación – EC, en el marco del cumplimiento de los requerimientos de la Guía de Acreditación de Entidades de Certificación vigente establecida por el INDECOPI.

3. 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.

4. 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). Los estándares mencionados se refieren a áreas como privacidad, seguridad, integridad de las transacciones, disponibilidad, confidencialidad y no repudio.

5. PARTICIPANTES

5.1. 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.

5.2. 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.

5.3. 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.

5.4. 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.

5.5. 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.

5.6. 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.

6. ALCANCE

El presente plan es de cumplimiento obligatorio por los proveedores de servicios de certificación digital contratados por SoftNet.

7. PLAN DE PRIVACIDAD DE DATOS

SoftNet garantiza la protección de datos personales de los suscriptores y titulares de los servicios de registro, en cumplimiento de la Ley de Protección de Datos Personales – Ley N°29733, la Norma Marco de Privacidad y la Guía de Acreditación de Entidades de Registro o Verificación, en los ámbitos legales, regulatorios y contractuales.

Serán considerados como datos personales, la información de nombres, dirección, correo electrónico, y toda información que pueda vincularse a la identidad de una persona natural o jurídica, contenidos en los contratos y solicitudes de los suscriptores y titulares. Esta información será considerada como confidencial y será de uso exclusivo para las operaciones de registro, a excepción que exista un previo consentimiento del titular de dichos datos o medie una orden judicial o administrativa que así lo determine.

Con este fin, se implementa el presente Plan de Privacidad con controles para la protección contra divulgación y uso no autorizado.

Es responsabilidad de los suscriptores garantizar que la información provista a SoftNet sea veraz y vigente. Asimismo, son responsables del perjuicio que pudieran causar por aportar datos falsos, incompletos o inexactos

7.1. INFORMACIÓN RECOLECTADA Y PROTEGIDA

Como parte de las operaciones de certificación, SoftNet recolecta información de los suscriptores y titulares del siguiente tipo:

- Datos de identificación personal, incluyendo la fotografía que aparece en su documento de identidad.
- Contrato de solicitud de servicios.

7.2. TRATAMIENTO DE LOS DATOS PERSONALES

Deberá considerarse como información no privada, la siguiente:

- Información personal públicamente disponible. En estos casos no será requerida autorización del usuario para dar publicidad a esta información.

Deberá considerarse como información privada, la siguiente:

- De conformidad con lo establecido por la Norma Marco sobre privacidad del APEC, se considera información personal, cualquier información relativa a un individuo identificado o identificable.

- Información que pueda permitir a personas no autorizadas la construcción de un perfil de las actividades de los usuarios de los servicios de sellado de tiempo.
- En todos los casos, figurará en la Política de Privacidad que deberá ser suscrita por el mismo, su consentimiento para el tratamiento y almacenamiento de estos datos.

La información personal considerada como privada únicamente será divulgada en caso que exista consentimiento previo y por escrito firmado para tales efectos por el titular de dicha información o medie una orden judicial o administrativa que así lo determine.
Cualquier violación a la privacidad de esta información por parte del personal de SoftNet o de los terceros subcontratados, será sujeto de sanción.

7.3. FLUJO TRANSFRONTERIZO DE DATOS PERSONALES

Los contratos de los suscriptores contendrán cláusulas que soliciten el consentimiento del suscriptor y titular de transferir los datos personales contenidos en el certificado digital a los países donde se encuentren las EC.

7.4. IMPLEMENTACIÓN DE LOS PRINCIPIOS DE PRIVACIDAD

El presente documento adopta lo establecido por el APEC a través de la Norma Marco sobre Privacidad respecto de los principios que deben ser observados siempre que se realice algún tipo de labor o función que involucre la recolección, posesión, procesamiento, uso, transferencia o revelación de información personal.

7.4.1. MEDIDAS PREVENTIVAS

a) Restringir el acceso a los datos personales a tan sólo el personal autorizado.
b) Proteger estos datos contra acceso no autorizado.
c) Concientizar al personal para no divulgar o exponer de manera accidental datos personales de los usuarios.
d) Implementar procedimientos para documentar las prácticas en lo que respecta a la información personal que se recolecta durante las actividades de operación o comercialización de los servicios de certificación, las mismas que deben informar sobre:
    i El hecho de que se está recolectando información personal.
    ii Los propósitos para los cuales se recolecta dicha información personal.
    iii Los tipos de personas u organizaciones a las que dicha información podría ser revelada.
    iv La identidad y ubicación del responsable de la información personal, incluyendo información respecto a la forma de contactarlo en razón a sus prácticas y manejo de la información personal.
    v Las opciones y medios que ofrece el responsable de la información personal a los individuos para limitar el uso y revelación, así como los mecanismos para el acceso y corrección de su información.
    vi Deben tomarse todos los pasos razonablemente necesarios, a fin de asegurar que se provee tal información, sea antes o en el mismo momento en que se está efectuando la recolección de la información personal. Caso contrario, deberá proveerse esta información tan pronto como sea factible.
e) Puede no resultar apropiado exigir que los responsables de la información personal provean información respecto a la recolección y uso de información que se encuentra públicamente disponible.

7.4.2. LIMITACIONES A LA RECOLECCIÓN

La recolección de información personal debe encontrarse limitada a la información que es relevante para el propósito para el cual se está recolectando y esta información deberá ser obtenida de manera legal y apropiada, y, en la medida de lo posible, con la debida información o consentimiento del individuo al cual pertenece.

7.4.3. USO DE LA INFORMACIÓN PERSONAL

a) La información personal recolectada será usada en estricto cumplimiento de los propósitos de la recolección o aspectos relativos a los mismos, excepto: vii. que exista consentimiento del individuo al que pertenece la información personal recolectada;
   - i que esta información fuera necesaria para la provisión de un servicio o producto solicitado por el individuo; o
   - ii que la recolección fuera permitida por mandato de ley u otros instrumentos legales o exista algún tipo de pronunciamiento con efectos legales que lo autorizara.

7.4.4. ELECCIÓN

a) Cuando sea apropiado, se proveerá a los individuos mecanismos claros, prominentes, fáciles de entender, accesibles y económicos a fin que puedan decidir respecto a la recolección, uso y revelación de su información personal.
   Puede no resultar necesario que los responsables de la información provean estos mecanismos en los casos de recolección de información que sea públicamente disponible.

7.4.5. INTEGRIDAD DE LA INFORMACIÓN PERSONAL

a) La información personal deberá ser exacta, completa y mantenerse actualizada en el extremo que fuere necesario para los propósitos de su empleo.

7.4.6. SALVAGUARDAS A LA SEGURIDAD

a) Los responsables de la información personal deberán proteger la información personal que mantienen, a través de salvaguardas apropiadas contra riesgos tales como pérdida de la información o acceso indebido a la misma, así como contra la destrucción, uso, modificación o revelación no autorizada o cualquier otro abuso. Estas salvaguardas deberán ser proporcionales a la naturaleza y gravedad del daño potencial, la sensibilidad de la información y el contexto en que ésta es mantenida, y deberán ser sometidas a revisiones y reevaluaciones periódicas.

7.4.7. ACCESO Y CORRECCIÓN

a) Los individuos deben ser capaces de:
   - i obtener del responsable de la información personal, la confirmación respecto a si mantiene o no información personal que les concierne.
   - ii comunicar su información personal, luego de haber probado suficientemente su identidad, dentro de un periodo de tiempo razonable; por una tarifa, si es que la hubiera, la cual no debe ser excesiva; de una manera razonable; de un formato que sea razonablemente comprensible; y iii. cuestionar la exactitud de la información que les concierne y de ser posible y apropiado, hacer que la información sea rectificada, completada, enmendada o borrada.

b) Debe proveerse acceso y oportunidad para la corrección de la información, salvo cuando:

i La carga o costo de hacerlo sea indebido o desproporcional a los riesgos de la privacidad individual en el caso en cuestión;
ii la información no pueda ser divulgada por razones legales o de seguridad o para proteger información comercial de carácter confidencial; o
iii se podría violar la privacidad de la información de personas diferentes al individuo.

c) Si una solicitud bajo el supuesto (a) o (b) o un cuestionamiento bajo el supuesto (c) es denegado, se debe informar al individuo las razones en las que se basa dicha denegatoria y se le debe informar respecto a los mecanismos para cuestionar dicha decisión.

7.5. RESPONSABILIDADES

El Responsable de Privacidad de SoftNet gestiona la implementación y vela por el cumplimiento del presente plan, así como de su revisión periódica, actualización, difusión y concientización y capacitación al personal y terceros para su adecuado cumplimiento.

7.6. CONFORMIDAD

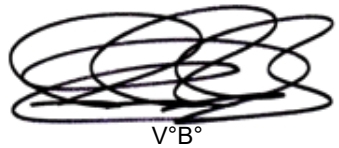
Este documento ha sido aprobado por el Responsable de la EC de SoftNet, y cualquier incumplimiento por parte de los empleados, contratistas y terceros mencionados en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.

8. HISTORIAL DE CAMBIOS

Generales			
Propietario del Documento	*Carlos Dextre*	Clasificación	*Privada*
Aprobado por:	*Carlos Dextre*	Fecha aprobación	*12/05/2020*

Fecha	*Versión*	*Descripcion*	*Autor*
12/05/2020	*1.0*	*Documento Inicial*	*Coordinador de Seguridad de la Información*
12/05/2020	*1.0*	*Revision de Documentos*	*Gerente de Productos y Servicios*
28/10/2020	*1.0*	*Revision de documentos*	*Gerente de Productos y Servicios*
12/06/2023	*1.1*	*Revision*	*CISO - Gerente SIG*
12/06/2023	*1.1*	*Revision de Documento*	*Gerente de Productos y Servicios*
12/06/2023	*1.1*	*Aprobacion*	*Representante de la EC*
10/06/2024	*1.1*	*Revision*	*CISO - Gerente SIG*
10/06/2024	*1.1*	*Revision de Documento*	*Gerente de Productos y Servicios*
10/06/2024	*1.1*	*Aprobacion*	*Representante de la EC*
14/11/2024	*1.2*	*Inclusion de OR-AC Alvaro Suarez y Marco Sanchez*	*CISO - Gerente SIG*
14/11/2024	*1.2*	*Revision de Documento*	*Jefe de Productos Servicios e Infraestructura Tecnologica*
14/11/2024	*1.2*	*Aprobacion*	*Representante de lña EC y ER*
01/07/2025	*1.3*	*Revision y Actualizacion de Responsable de EC*	*Oficial de Privacidad – CISO GSIG*
01/07/2025	*1.3*	*Revision*	*Oficial De Seguridad – Jefe de PSIT*
01/07/2025	*1.3*	*Aprobación*	*Responsable de EC – Representante Legal*

Fecha	*Versión*	*Descripcion*	*Autor*

Elaborado por: Pedro Rivera P.	Revisado y Aprobado por: Mario J. Sanchez B.	Revisado y Aprobado por: Leonel Garcia Jauregui
 V°B°	 V°B°	 V°B°
Cargo: Oficial de Privacidad – CISO GSIG	Cargo: Oficial de Seguridad - Jefe de PSIT	Cargo: Responsable de la EC

Firmado Digitalmente por:
LEONEL GARCIA JAUREGUI
Fecha: 24/07/2025 16:19:23