ENTIDAD DE REGISTRO O VERIFICACIÓN

POLÍTICA DE REGISTRO

VERSIÓN 1.0

CONTENIDO

1. INTRODUCCIÓN 3

2. OBJETIVO DE SOFTNET COMO ENTIDAD DE REGISTRO O VERIFICACIÓN. 3

3. PARTICIPANTES 3

3.1. ENTIDAD DE CERTIFICACIÓN 3
3.2. ENTIDAD DE REGISTRO O VERIFICACIÓN 3
3.3. PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL 3
3.4. TITULAR 4
3.5. SUSCRIPTOR 4
3.6. TERCERO QUE CONFÍA 4

4. DEFINICIONES Y ABREVIACIONES 4

5. USO APROPIADO DEL CERTIFICADO 6

6. ADMINISTRACIÓN DE POLÍTICAS 6

6.1. ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DE RPS 6
6.2. PROCEDIMIENTO DE APROBACIÓN DE RPS 6

7. PUBLICACIÓN Y REGISTRO 6

7.1. PUBLICACIÓN DE LA INFORMACIÓN SOBRE CERTIFICACIÓN 6
7.2. TIEMPO O FRECUENCIA DE LA PUBLICACIÓN 6
7.3. CONTROLES DE ACCESO A LOS REGISTROS 6

8. IDENTIFICACIÓN Y AUTENTICACIÓN 7

9. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADOS 7

10. CONTROLES DE LAS INSTALACIONES, DE LA GESTION Y CONTROLES OPERACIONALES 7

10.1. CONTROLES FÍSICOS 7
10.2. CONTROLES PROCESALES 7
10.3. CONTROLES DE PERSONAL 8
10.4. PROCEDIMIENTO DE REGISTRO DE AUDITORÍAS 8
10.5. ARCHIVO DE REGISTRO 8
10.6. RECUPERACIÓN FRENTE AL COMPROMISO Y DESASTRE 8
10.7. FINALIZACIÓN DE LA ER 8

11. AUDITORIAS DE COMPATIBILIDAD Y OTRAS EVALUACIONES 8

12. OTRAS MATERIAS DE NEGOCIO Y LEGALES 9

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).

2. OBJETIVO DE SOFTNET COMO ENTIDAD DE REGISTRO O VERIFICACIÓN.

Asegurar la confiabilidad de la identidad del solicitante de los servicios de emisión, revocación y suspensión de los certificados digitales, registrando y verificando la información entregada por los solicitantes antes de comunicar a la Entidad de Certificación la aprobación de una solicitud. Y dar cumplimiento a las normas, políticas y directrices establecidos por cada EC con las que tenga convenio, para sus Entidades de Registro a nivel internacional.

3. PARTICIPANTES

3.1. 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.

3.2. 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.

3.3. 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.

3.4. 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.

3.5. 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.

3.6. 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.

4. 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.

5. USO APROPIADO DEL CERTIFICADO

Los criterios para definir el uso apropiado, rango de acción o aplicabilidad de un certificado digital solicitado a la ER de SoftNet depende de lo establecido en la Política de Certificación y Declaración de Prácticas de cada EC con la cual tenga convenio, para cada tipo de certificado.

6. ADMINISTRACIÓN DE POLÍTICAS

6.1. ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DE RPS

Los detalles de contacto están registrados en la RPS de SoftNet.

6.2. PROCEDIMIENTO DE APROBACIÓN DE RPS

INDECOPI, en su calidad de Autoridad Administrativa Competente (AAC), aprueba la RPS de la ER de SoftNet luego de ejecutados los procedimientos establecidos en la Guía de Acreditación de Entidades de Registro y comprobada su correcta observancia.

7. PUBLICACIÓN Y REGISTRO

7.1. PUBLICACIÓN DE LA INFORMACIÓN SOBRE CERTIFICACIÓN

La Declaración de Prácticas de Registro y toda la documentación pertinente y relevante vigente de la ER de SoftNet, así como sus versiones anteriores, son publicadas en la siguiente dirección web:

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

7.2. TIEMPO O FRECUENCIA DE LA PUBLICACIÓN

Las modificaciones relativas a la RPS u otra documentación de la ER de SoftNet son publicadas tan pronto como razonablemente sea posible, debiendo tener cuidado de cumplir con los requisitos que fueren necesarios para la aprobación de dichas modificaciones.
Toda modificación relativa a la RPS debe ser aprobada por INDECOPI antes de su publicación.

7.3. CONTROLES DE ACCESO A LOS REGISTROS

El acceso a los registros debe ser restringido únicamente para el uso de los titulares y suscriptores legítimos, así como a los trabajadores competentes dentro de la ER de SoftNet, teniendo en cuenta los temas de privacidad que pudieran existir en los contratos de los suscriptores o titulares y en conformidad con la Norma Marco sobre Privacidad.
Se debe emplear sistemas fiables para el registro, de modo tal que:

- Únicamente personas autorizadas tengan acceso a lectura y modificaciones.

- Pueda comprobarse la autenticidad de la información.

8. IDENTIFICACIÓN Y AUTENTICACIÓN

La RPS de SoftNet describe los procedimientos y criterios utilizados para autenticar la identidad y/o otros atributos de un solicitante de certificado, mediante la verificación presencial de la identidad del solicitante. Además, se describen los procedimientos para autenticar las partes que soliciten otros servicios como revocación o suspensión de certificado (la habilitación de los últimos tres procesos mencionados dependerá de lo establecido por cada EC en su respectiva CPS para la cual se brinde el servicio de ER). En el caso del proceso de solicitud de revocación de un certificado, se requerirá la presencia física del solicitante para todos los casos en los que dicho solicitante es una persona distinta al suscriptor del certificado (titulares, terceros o representantes legalmente autorizados). Los suscriptores podrán también presentarse en la ER para realizar sus solicitudes, pero dicha acción no será obligatoria a menos que la EC no establezca en su CPS otros mecanismos de solicitud (por ejemplo, a través de mecanismos telemáticos).
En los casos que los certificados sean emitidos para ser usados por agentes automatizados, el proceso de validación para la vinculación entre el certificado y el agente es establecido en esta RPS.
La EC asociada debe establecer el procedimiento para la prueba de posesión de la clave privada y su almacenamiento en módulos acreditados según el Common Criteria, FIPS 140-2 o equivalente, con la declaración del número de serie del módulo, factura o auditoría respectiva, por ejemplo.

9. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADOS

El ciclo de vida de un certificado personal no debe exceder el periodo establecido por la IOFE, el mismo que será de máximo tres (3) años de acuerdo con la legislación vigente.
La RPS de la ER de SoftNet define los procedimientos que podrán ser empleados al solicitar los servicios de la ER, vale decir emisión, revocación y suspensión de certificados.

10. CONTROLES DE LAS INSTALACIONES, DE LA GESTION Y CONTROLES OPERACIONALES

10.1. CONTROLES FÍSICOS

Los controles físicos que deben ser implementados son descritos en el documento Política de Seguridad de la ER de SoftNet.

10.2. CONTROLES PROCESALES

Los controles implementados para la gestión de roles son descritos en el documento Política de Seguridad de la ER de SoftNet.

10.3. CONTROLES DE PERSONAL

Los controles implementados para la gestión del personal son descritos en el documento Política de Seguridad de la ER de SoftNet.

10.4. PROCEDIMIENTO DE REGISTRO DE AUDITORÍAS

Los procedimientos implementados para el registro de auditorías son descritos en el documento Política de Seguridad de la ER de SoftNet.

10.5. ARCHIVO DE REGISTRO

Los controles implementados para la gestión del archivo son descritos en el documento Política de Seguridad de la ER de SoftNet.

10.6. RECUPERACIÓN FRENTE AL COMPROMISO Y DESASTRE

Se establece un plan de contingencias que permita el restablecimiento y mantenimiento de las operaciones de la ER. Este plan contempla las acciones a realizar, los recursos a utilizar y el personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación.

10.7. Finalización de la ER

La ER informará al INDECOPI, a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con por lo menos treinta (30) días calendario de anticipación.
Se debe asegurar que todos los datos necesarios para la continuación de las operaciones bajo el marco de la IOFE son transferidos al propio INDECOPI o a otro PSC designado por éste.
Si fuera el caso de una operación de transferencia de titularidad, se debe asegurar que los nuevos dueños u operadores cumplan con los requisitos de acreditación.

11. AUDITORIAS DE COMPATIBILIDAD Y OTRAS EVALUACIONES

Se debe estar sometido a auditoría de compatibilidad independiente en relación con las operaciones que realiza. La frecuencia de auditorías externas o evaluaciones de compatibilidad y el proceso de publicación de los resultados debe ser de una vez al año.
La auditoría de compatibilidad o los procesos de evaluación requeridos para obtener y mantener la acreditación están establecidos en la RPS y en la Política de Seguridad.

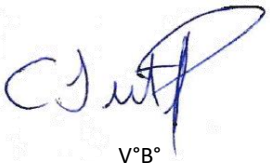
12. OTRAS MATERIAS DE NEGOCIO Y LEGALES

Estas serán descritas en la RPS.

HISTORIAL DE CAMBIOS

Generales			
Propietario del Documento	*Carlos Dextre*	**Clasificación**	*Privada*
Aprobado por:	*Carlos Dextre*	**Fecha aprobación inicial**	*15/09/2020*

Historial de Versiones			
Fecha	**Versión**	**Resumen de Cambios**	**Autor**
01/08/2020	1.0	Documento Inicial	Oficial de Seguridad
15/09/2020	1.0	Aprobación	Responsable de ER

Elaborado por: Pedro Rivera P.	Revisado y Aprobado por: Christian Gutierrez P.	Revisado y Aprobado por: Carlos Dextre P.
 V°B°	 V°B°	 V°B°
Cargo: Responsable de Seguridad	Cargo: Gerente de Operaciones	Cargo: Responsable de la ER