SOLO PARA USO REFERENCIAL
ESTE DOCUMENTO ES SOLO PARA LECTURA EN WEB
ESTA PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

SOFTNET

PLAN DE CONTINGENCIA Y RECUPERACIÓN

Firmado Digitalmente por: PEDRO EMILIO RIVERA PEREZ
Fecha: 17/11/2022 11:45:21

CONTENIDO

SOLO PARA USO REFERENCIAL
ESTE DOCUMENTO ES SOLO PARA LECTURA EN WEB
ESTA PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL

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. PARTICIPANTES

2.1. 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.

2.2. 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.

2.3. 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.

ESTE DOCUMENTO ES SOLO PARA LECTURA EN WEB
ESTA PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL
SOLO PARA USO REFERENCIAL

2.4. 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.

2.5. 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 corresponderá 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.

2.6. 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.

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.

ESTE DOCUMENTO ES SOLO PARA USO REFERENCIAL
ESTA PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL
SOLO PARA LECTURA EN WEB

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 corresponderá 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.

ESTE DOCUMENTO ES SOLO PARA LECTURA EN WEB
ESTA PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL
SOLO PARA USO REFERENCIAL

4. ALCANCE

La presente política es de cumplimiento obligatorio para el personal contratado por la ER de SoftNet que participan de las operaciones críticas de los servicios de registro descritos en la Declaración de Prácticas de Registro.

5. PLAN DE CONTINGENCIA Y RECUPERACIÓN ANTE DESASTRES

La ER de SoftNet mantiene un plan de contingencias que define acciones, recursos y personal para el restablecimiento y mantenimiento de las operaciones de registro de los procesos de atención de solicitudes de emisión y revocación, en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación.

En caso la EC asociada sufra de algún tipo de desastre, ésta debe contar con un Plan de Contingencia que inmediatamente entre en acción. La recuperación de los sistemas administrados por la EC asociada, incluyendo la disponibilidad de los sistemas de registro, que permiten la comunicación entre la ER de SoftNet y la EC asociada, es responsabilidad de dicha EC. En esos casos, la ER de SoftNet informará a los titulares y suscriptores el hecho mediante un mensaje de correo electrónico.

Los planes son evaluados por lo menos una vez durante el periodo de cada auditoría o evaluación de compatibilidad y los resultados deben ser puestos a disposición de los auditores de compatibilidad o asesores, juntamente con la información respecto a las acciones correctivas que pudieran ser necesarias.

Se definen las acciones a tomar para recuperación ante la ocurrencia de un desastre. Este Plan de Recuperación contiene 3 etapas:

5.1. ACTIVIDADES PREVIAS AL DESASTRE

Como actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de información que nos asegure un proceso de recuperación con el menor costo posible a nuestra institución, tenemos que señalar las siguientes acciones que son precisas de realizar en la ejecución del presente plan.

5.1.1. Definición y Establecimiento de un Plan de Acción

Establecer los procedimientos relativos a:

(1). **Plataforma de la Entidad de Registro.** La EC asociada proporciona la plataforma informática para el desarrollo de las actividades de la ER de SoftNet, así como el soporte respectivo. Los procedimientos para recuperación ante desastres provistos por EC asociada garantizan el pronto restablecimiento del servicio.

(2). **Equipos de Cómputo**. Dado que el acceso a la plataforma informática de la EC asociada es vía web y utilizando un certificado digital para el Operador de Registro, el equipo de cómputo puede ser reemplazado sin problemas en caso de verse comprometido.

(3). **Certificado Digital para el Operador de Registro.** Este documento es la única credencial válida que puede usar el Operador de Registro para autenticarse con la plataforma informática de la EC asociada. En caso de compromiso, éste debe ser revocado y reemplazado por uno nuevo.

(4). **Unidad de Almacenamiento para la documentación recopilada durante el proceso de registro.** Dicha unidad se encuentra custodiada en una caja fuerte que lo protege contra la humedad y el fuego. En caso de pérdida se recurrirá a la información almacenada en la nube privada de SoftNet que se encuentra en el data center contratado con CenturyLink, la replicación de la información en esta nube será de manera mensual.

ESTE DOCUMENTO ES SOLO PARA USO REFERENCIAL
SOLO PARA LECTURA EN WEB
ESTA PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL

5.2. ACTIVIDADES POSTERIORES AL DESASTRE

El Responsable de la Entidad de Registro es la persona encargada de poner en práctica el Plan de Contingencia y Recuperación ante Desastres. Se realizarán algunas de las siguientes actividades.

5.3. EVALUACIÓN DE DAÑOS

Inmediatamente después que la contingencia ha concluido, se evaluará la magnitud de los daños producidos, estableciendo que sistemas están afectados, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.
Adicionalmente se lanzará un pre-aviso a la EC asociada, para ir avanzando en las labores de preparación de la ejecución de las actividades del Plan de Contingencia.

5.4. PRIORIZACIÓN DE ACTIVIDADES DEL PLAN DE ACCIÓN

Toda vez que el Plan de acción contemple una pérdida total, la evaluación de daños reales y su comparación con el Plan, nos dará la lista de actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra Entidad de Registro.
Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, para su asignación temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

5.5. EJECUCIÓN DE ACTIVIDADES

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el Plan de acción.
Cada uno de estos equipos contará con un coordinador que reportará diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, informará de inmediato al Responsable de la Entidad de Registro.
Las actividades por realizar son las siguientes:

- Contactarse con la EC asociada para coordinar la aplicación de su Plan de Contingencia.
- Contactarse con la EC asociada para revocar el certificado del Operador de Registro y emitir uno nuevo.
- Contactarse con el proveedor de acceso a internet para restablecer el servicio o reemplazarlo por un enlace inalámbrico si fuera necesario.

5.5.1. Evaluación de Resultados.

Una vez concluidas las labores de recuperación del (los) sistema(s) que fueron afectados por la contingencia, se evaluará objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.
De la evaluación de resultados y del siniestro, saldrán dos tipos de recomendaciones, una la retroalimentación del Plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

ESTE DOCUMENTO ES SOLO PARA LECTURA EN WEB
SOLO PARA USO REFERENCIAL
ESTA PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

5.6. RETROALIMENTACIÓN DEL PLAN DE ACCIÓN

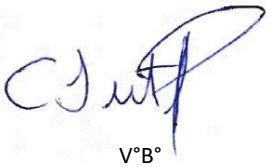
Con la evaluación de resultados, se optimizará el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

SOLO PARA USO REFERENCIAL
ESTE DOCUMENTO ES SOLO PARA LECTURA EN WEB
ESTA PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL

6. HISTORIAL DE CAMBIOS

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

Fecha	Versión	Resumen de Cambios	Autor
01/08/2020	*1.0*	*Documento Inicial*	*Coordinador de Seguridad de la Información*
15/09/2020	*1.0*	*Revisión de Documentos*	*Gerente de Productos y Servicios*
15/09/2020	*1.0*	*Aprobación*	*Respresentante de la 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: Coordinador de Seguridad de la Información	Cargo: Gerente de Productos y Servicios	Cargo: Gerente General Responsable de la ER

ESTE DOCUMENTO ES SOLO PARA USO REFERENCIAL
SOLO PARA LECTURA EN WEB
ESTA PROHIBIDA SU REPRODUCCION TOTAL O PARCIAL