POLITICA DE SEGURIDAD

Firmado digitalmente por PEDRO EMILIO RIVERA PEREZ
Fecha: 2021.11.19 14:54:43 -05'00'

CONTENIDO

1. INTRODUCCIÓN 4

2. OBJETIVO DE SOFTNET COMO ENTIDAD DE REGISTRO O VERIFICACIÓN 4

3. PARTICIPANTES 4

3.1. ENTIDAD DE CERTIFICACIÓN 4
3.2. ENTIDAD DE REGISTRO O VERIFICACIÓN 4
3.3. PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL 4
3.4. TITULAR 5
3.5. SUSCRIPTOR 5
3.6. TERCERO QUE CONFÍA 5

4. DEFINICIONES Y ABREVIACIONES 5

5. ALCANCE 6

6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 6

7. SEGURIDAD FÍSICA 7

7.1. UBICACIÓN Y CONSTRUCCIÓN DEL LOCAL 7
7.2. SEGURIDAD FÍSICA DEL PERSONAL Y EL EQUIPAMIENTO 7
7.3. PERÍMETROS DE SEGURIDAD Y CONTROL DE ACCESO FÍSICO 7
7.4. PROTECCIÓN CONTRA LA EXPOSICIÓN AL AGUA 7
7.5. PROTECCIÓN CONTRA INCENDIOS 7
7.6. ARCHIVO DE MATERIAL 8
7.7. GESTIÓN DE RESIDUOS 8
7.8. COPIA DE SEGURIDAD EXTERNA 8

8. SEGURIDAD DE COMUNICACIONES Y REDES 8

9. CONTROL DE CAMBIOS Y CONFIGURACIÓN 8

10. GESTIÓN DE ROLES 9

10.1. ROLES DE CONFIANZA 9
10.2. NÚMERO DE PERSONAS REQUERIDAS POR LABOR 9
10.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL 9
10.4. ROLES QUE REQUIEREN FUNCIONES POR SEPARADO 9

11. GESTIÓN DEL PERSONAL 10

11.1. CUALIDADES Y REQUISITOS, EXPERIENCIA Y CERTIFICADOS 10
11.2. PROCEDIMIENTO PARA VERIFICACIÓN DE ANTECEDENTES 10
11.3. REQUISITOS DE CAPACITACIÓN 10
11.4. FRECUENCIA Y REQUISITOS DE LAS RE-CAPACITACIONES 10
11.5. FRECUENCIA Y SECUENCIA DE LA ROTACIÓN EN EL TRABAJO 10
11.6. SANCIONES POR ACCIONES NO AUTORIZADAS 10
11.7. REQUERIMIENTOS DE LOS CONTRATISTAS 11
11.8. DOCUMENTACIÓN SUMINISTRADA AL PERSONAL 11

12. PROCEDIMIENTOS DE REGISTRO DE AUDITORÍAS 11

12.1. TIPOS DE EVENTOS REGISTRADOS 11
12.2. FRECUENCIA DEL PROCESAMIENTO DEL REGISTRO 11

12.3. PERIODO DE CONSERVACIÓN DEL REGISTRO DE AUDITORÍAS 11
12.4. PROTECCIÓN DEL REGISTRO DE AUDITORÍA 12
12.5. COPIA DE SEGURIDAD DEL REGISTRO DE AUDITORÍA 12
12.6. AUDITORÍA Y DETECCIÓN DE INTRUSIONES 12
12.7. NOTIFICACIÓN AL TITULAR QUE CAUSA UN EVENTO 12
12.8. VALORACIÓN DE VULNERABILIDAD 12

13. MEDIOS DE ALMACENAMIENTO 12

14. ARCHIVO 13

14.1. PROTECCIÓN DEL ARCHIVO 13
14.2. PROCEDIMIENTO PARA OBTENER Y VERIFICAR LA INFORMACIÓN DEL ARCHIVO 13

15. RECUPERACIÓN FRENTE AL COMPROMISO Y DESASTRE 13

15.1. PLAN DE CONTINGENCIAS 13
15.2. COMPROMISO DE LA CLAVE PRIVADA 13

16. CONFIDENCIALIDAD DE INFORMACIÓN DE LA ER 14

16.1. INFORMACIÓN CONSIDERADA CONFIDENCIAL 14
16.2. INFORMACIÓN QUE PUEDE SER PUBLICADA 14

17. RESPONSABILIDADES 14

18. CONFORMIDAD 14

19. HISTORIAL DE CAMBIOS 15

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 EC asociada, la aprobación de una solicitud.

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. 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.

6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La ER de SoftNet tiene como objetivo de seguridad, garantizar la autenticidad e integridad de la información crítica de los procesos de registro, mediante la gestión de riesgos de seguridad y la aplicación de políticas y estándares que regulen las actividades críticas de las operaciones de sellado de tiempo, por parte del personal y terceros subcontratados, en cumplimiento de las obligaciones de la ER en los ámbitos legales, regulatorios y contractuales.

7. SEGURIDAD FÍSICA

7.1. UBICACIÓN Y CONSTRUCCIÓN DEL LOCAL

La ubicación y diseño de las instalaciones de la ER de SoftNet debe prever el daño por desastres naturales, como inundación, terremoto; así como desastres creados por el hombre, como incendios, disturbios civiles y otras formas de desastre, manteniendo vigente su acreditación ante el Instituto Nacional de Defensa Civil.

7.2. SEGURIDAD FÍSICA DEL PERSONAL Y EL EQUIPAMIENTO

A fin de proteger al personal y el equipamiento en las instalaciones de la ER de SoftNet se implementan medios que garanticen la seguridad física de los equipos y del personal. Se tienen los siguientes controles:

a) Señalización de zonas seguras.
b) Provisión de extinguidores contra incendios.
c) No debe existir cableado eléctrico expuesto.
d) Uso de estabilizadores y supresores de picos.

7.3. PERÍMETROS DE SEGURIDAD Y CONTROL DE ACCESO FÍSICO

Las áreas de archivo de documentos en papel y archivos electrónicos deben estar protegidas constantemente contra acceso no autorizado:

a) Deben estar en ambientes separados de las áreas públicas de registro.
b) Sólo debe ingresar personal autorizado.
c) El ingreso y salida del personal debe ser registrado.
d) Los terceros y el personal de limpieza pueden ingresar con autorización del Responsable de Seguridad, deben ser previamente identificados y deben ser registrados y supervisados durante su estancia en el área.
e) El ingreso y salida de documentos debe ser registrada.
f) Debe estar cerrada bajo llave cuando no esté siendo usada.
g) Cuando sea asignado un personal nuevo se deberán verificar sus antecedentes.

Las operaciones de validación y registro pueden realizarse en las instalaciones de la ER de SoftNet o en las instalaciones del cliente o cualquier otro lugar definido por él en presencia del Operador de Registro, el cual será responsable de proteger la información proporcionada por el cliente.

7.4. PROTECCIÓN CONTRA LA EXPOSICIÓN AL AGUA

Las instalaciones deben estar protegidas contra exposición al agua, en particular, las áreas de archivo deben estar distantes de zonas de filtración de agua o humedad, ya sea en el techo o en las paredes colindantes.

7.5. PROTECCIÓN CONTRA INCENDIOS

Las instalaciones deben poseer las siguientes medidas para la prevención y protección contra incendios:

a) Está prohibido fumar o generar cualquier fuente de humo o fuego dentro de las áreas de archivo y en las instalaciones de SoftNet en calidad Entidad de Registro.
b) Se debe contar con un extinguidor visible, destinado a extinguir fuego sobre equipos electrónicos y documentos en papel.
c) Una copia de los documentos y archivos electrónicos, que poseen las solicitudes de los servicios de registro y los contratos de los titulares y suscriptores debe ser guardada en un lugar de contingencia protegida por el Responsable de la ER, contra acceso no autorizado

7.6. ARCHIVO DE MATERIAL

Los archivos tanto electrónicos como de papel (contratos de suscriptores y solicitudes de los servicios de registro) y el material distintivo (formatos membretados propios de la ER), deben estar protegidos en las áreas de archivo, en contenedores de protección contra fuegos y deben situarse en diversas dependencias para eliminar riesgos asociados a una única ubicación.
El acceso a estos contenedores debe estar restringido a personal autorizado.

7.7. GESTIÓN DE RESIDUOS

Los archivos tanto electrónicos como de papel (contratos de suscriptores y solicitudes de los servicios de registro) y el material distintivo (formatos membretados propios de la ER), que requieran ser eliminados o su soporte electrónico requiera ser desechado, deberán ser borrados o destruidos de manera irrecuperable.

7.8. COPIA DE SEGURIDAD EXTERNA

Una copia de los documentos y archivos electrónicos, que poseen las solicitudes de los servicios de registro y los contratos de los titulares y suscriptores debe ser guardada en un lugar de contingencia protegida por el Responsable de la ER, contra acceso no autorizado.

8. SEGURIDAD DE COMUNICACIONES Y REDES

Se deben establecer responsabilidades y procedimientos documentados de operación asociado al procesamiento de información y recursos de comunicaciones, con el objetivo de evitar daños, accesos no autorizados, mal uso de los activos de información, garantizar la seguridad de los datos y la disponibilidad de los servicios utilizados a través de la red de SoftNet y del internet.
En lo posible se segregarán las tareas y se implementará un procedimiento de gestión de cambios, con la finalidad de prevenir modificaciones no autorizadas en los equipos de comunicaciones y redes.
La ER de SoftNet asegurará que los datos disponibles en los repositorios públicos se encuentren protegidos, así como, deberá garantizar la disponibilidad de estos.

9. CONTROL DE CAMBIOS Y CONFIGURACIÓN

Se deben establecer un control satisfactorio de todos los cambios realizados a los equipos, software y procedimientos, en lo posible se deberá garantizar la posibilidad de revertir los cambios efectuados sin éxito.

Se deberá realizar y aprobar los cambios en los sistemas y recursos de tratamiento de información, de acuerdo a lo establecido; así mismo, previo al cambio se efectuará un análisis de impacto a los sistemas y procesos, comunicando el cambio a todos los involucrados

10. GESTIÓN DE ROLES

10.1. ROLES DE CONFIANZA

Los roles de confianza deben ser definidos de la siguiente manera:

- Responsable de la ER
- Responsable de Seguridad
- Responsable de Privacidad
- Operadores de Registro
- Asistente de Verificación de Identidad
- Auditores

Estos roles deben ser asignados formalmente por el Responsable de SoftNet en calidad Entidad de Registro.
La descripción de los roles debe incluir las labores que pueden como las que no pueden ser realizadas en el ejercicio de tales roles, las mismas que deben ser puestas de manifiesto a las personas que ejercen dichas funciones. Se debe obtener constancia por escrito del conocimiento de las mismas.

10.2. NÚMERO DE PERSONAS REQUERIDAS POR LABOR

Los cambios en los documentos normativos requieren de la autorización del Responsable de la ER, el Responsable de Seguridad y el de Privacidad. Dichos roles no son incompatibles y pueden ser asumidos por un mismo cargo.
El auditor deberá ser siempre una persona independiente de las operaciones de registro.

10.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Los roles de confianza deben emplear controles de acceso físico para el acceso a las áreas de archivo, así como lógicos para las comunicaciones con la EC. Los controles de acceso a los sistemas de Registro dependen de la configuración de los sistemas de cada EC asociada y no de la ER de SoftNet.

10.4. ROLES QUE REQUIEREN FUNCIONES POR SEPARADO

El auditor asignado por el INDECOPI deberá ser siempre una persona independiente de las operaciones de registro.

11. GESTIÓN DEL PERSONAL

11.1. CUALIDADES Y REQUISITOS, EXPERIENCIA Y CERTIFICADOS

Los roles de confianza deben tener conocimiento y entrenamiento en las operaciones de registro digital, la Política de Seguridad de la Información y la Política y el Plan de Privacidad de Datos. Asimismo, deben tener experiencia relacionada a los temas de certificación digital.

11.2. PROCEDIMIENTO PARA VERIFICACIÓN DE ANTECEDENTES

Se deben verificar los antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes vigentes y normatividad pertinente, que participan y tienen acceso a las operaciones y sistemas de registro, incluyendo:

- Verificación de antecedentes criminales
- Verificación de antecedentes crediticios

Las personas que desempeñan roles de confianza deben de tener en claro el nivel de sensibilidad y valor de los bienes y transacciones protegidos por la actividad de la cual ellas son responsables.

11.3. REQUISITOS DE CAPACITACIÓN

Todos los empleados de la organización que participan de los servicios de registro deben recibir las capacitaciones apropiadas y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral:

- El equipo y software requerido para operar.
- Los aspectos de la RPS, Política de Seguridad, Plan de privacidad y otra documentación relevante que afecte sus funciones.
- Requisitos legislativos en relación a sus funciones.
- Sus roles en relación con el Plan de Contingencias.

11.4. FRECUENCIA Y REQUISITOS DE LAS RE-CAPACITACIONES

Las sesiones de capacitación y entrenamiento deben ser llevadas a cabo anualmente y cuando existan cambios significativos en los elementos tratados en la capacitación inicial y cada vez que se adhiera, sustituya o rote al personal encargado.

11.5. FRECUENCIA Y SECUENCIA DE LA ROTACIÓN EN EL TRABAJO

No se implementará rotación de los trabajadores.

11.6. SANCIONES POR ACCIONES NO AUTORIZADAS

Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad, una acción real o potencial no autorizada y que haya sido realizada por una persona que desempeña un rol de confianza, dicha persona debe ser inmediatamente suspendida de todo rol de confianza que pudiera desempeñar.
Dichas sanciones deben estar establecidas en los contratos de cada empleado y/o contratista.

11.7. REQUERIMIENTOS DE LOS CONTRATISTAS

El personal contratado, para fines específicos dentro de las operaciones de la ER de SoftNet, será evaluado respecto de sus antecedentes criminales, conocimiento y experiencia. Asimismo, no deberá tener acceso sin supervisión a las áreas de archivo y no tendrá acceso a los sistemas de registro brindados por la EC.
Entre los requisitos de contratación de terceros está el conocimiento de las Políticas de Seguridad y la firma de un Acuerdo de Confidencialidad sobre la información que sea suministrada o conocida

11.8. DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

La documentación mencionada en el numeral 11.3 REQUISITOS DE CAPACITACIÓN, es entregada durante la capacitación de inducción y está publicada en la intranet para fácil consulta.

12. PROCEDIMIENTOS DE REGISTRO DE AUDITORÍAS

12.1. TIPOS DE EVENTOS REGISTRADOS

Los sistemas de información sensible son provistos por la EC asociada, por lo que la ER de SoftNet sólo puede acceder vía web. En este sentido, los logs de auditoría son administrados y definidos por la EC asociada.
Se guardarán los contratos de los titulares y suscriptores, así como las solicitudes de los procesos de registro, como evidencia de las transacciones realizadas y para efectos de auditoría.
La ER de SoftNet genera reportes de los siguientes eventos:

- Acceso físico a las áreas sensibles.
- Cambios en el personal.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte al sistema de certificación.

El registro de auditoría de eventos debe registrar la hora, fecha e identificadores software/hardware.

12.2. FRECUENCIA DEL PROCESAMIENTO DEL REGISTRO

Los registros de auditoría deben ser procesados y revisados una vez al mes como mínimo con el fin de buscar actividades sospechosas o no habituales.
El procesamiento de los registros de auditoría debe incluir la verificación de que dichos registros no hayan sido manipulados

12.3. PERIODO DE CONSERVACIÓN DEL REGISTRO DE AUDITORÍAS

Como mínimo los contratos de suscriptores y titulares, así como las solicitudes de los procesos de registro deben conservarse por un periodo de diez (10) años.

12.4. PROTECCIÓN DEL REGISTRO DE AUDITORÍA

Las áreas de archivo donde se almacenan los contratos de los suscriptores y los titulares, así como las solicitudes de los procesos de registro estarán protegidos contra acceso no autorizado y los ingresos y salidas de personal serán registrados.
La destrucción de un archivo de auditoría solo se podrá llevar a cabo con la autorización de INDECOPI, siempre y cuando haya transcurrido un periodo mínimo de 10 años.

12.5. COPIA DE SEGURIDAD DEL REGISTRO DE AUDITORÍA

Todas las solicitudes y contratos físicos serán generados con copia y los documentos electrónicos tendrán una copia por los Operadores de Registro. Las copias serán almacenadas en un lugar diferente como contingencia, protegidas contra acceso no autorizado por el Responsable de la ER de SoftNet.

12.6. AUDITORÍA Y DETECCIÓN DE INTRUSIONES

Las auditorías internas se llevarán a cabo al menos una vez al año en la ER de SoftNet.
Las evaluaciones técnicas del INDECOPI se llevarán llevarse a cabo una vez al año y cada vez que el INDECOPI lo requiera.
La plataforma de la ER de SoftNet está a cargo de su proveedor de servicios de certificación, eMudhra quien es responsable su mantenimiento, incluyendo las pruebas periódicas de detección de intrusiones.

12.7. NOTIFICACIÓN AL TITULAR QUE CAUSA UN EVENTO

Las notificaciones automáticas dependen de los sistemas de la EC, para todos los eventos relacionados con el uso de los certificados por parte de un titular.

12.8. VALORACIÓN DE VULNERABILIDAD

Los sistemas de registro son administrados por cada EC asociada, por lo que la protección perimetral de redes corresponde a la infraestructura de cada EC certificada con el sello de WebTrust.

13. MEDIOS DE ALMACENAMIENTO

Se debe asegurar la protección de los documentos, medios informáticos, datos de entrada o salida y documentación del proceso de validación de identidad, de las ocurrencias como daño, modificación, robo o acceso no autorizado.
Se debe establecer un procedimiento para la administración de los medios de almacenamiento de información, y los controles de seguridad requeridos para el almacenamiento, uso y protección de la información, considerándose también el uso de los medios de almacenamiento removibles, el proceso de eliminación segura de información, la planificación y ejecución de copias de seguridad, así como su proceso de restauración.

14. ARCHIVO

14.1. PROTECCIÓN DEL ARCHIVO

El archivo físico está protegido con controles de acceso físico para impedir el acceso a personas no autorizadas. Los documentos deben estar firmados de manera manuscrita y digital respectivamente para prevenir cualquier modificación.
El ingreso y salida de documentos físicos y digitales debe ser registrado para impedir la pérdida o destrucción no autorizada.
Debe tomarse en consideración la posibilidad de re-firmado de los archivos cuando los avances en las tecnologías generen potencialmente una posibilidad de afectación a los mismos o la generación de microformas según Decreto Legislativo 681.

14.2. PROCEDIMIENTO PARA OBTENER Y VERIFICAR LA INFORMACIÓN DEL ARCHIVO

Mensualmente, la integridad del archivo debe ser verificada.

15. RECUPERACIÓN FRENTE AL COMPROMISO Y DESASTRE

15.1. PLAN DE CONTINGENCIAS

La ER de SoftNet mantiene un plan de contingencias que define acciones, recursos y personal para el restablecimiento y mantenimiento de las operaciones 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.
El plan asegura que los servicios de registro para los procesos de emisión y revocación, puedan ser reasumidos dentro de un plazo máximo de 24 horas
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.
La recuperación de los sistemas administrados por la EC, incluyendo la disponibilidad de los sistemas de registro, que permiten la comunicación entre la ER y la EC, es responsabilidad de la EC asociada. En esos casos, la ER de SoftNet informará a los titulares y suscriptores el hecho mediante un mensaje de correo electrónico.

15.2. COMPROMISO DE LA CLAVE PRIVADA

En el caso de compromiso de la clave privada de un empleado que cumpla un rol de confianza, el certificado deberá ser revocado y se deberá solicitar la emisión de un nuevo certificado.

16. CONFIDENCIALIDAD DE INFORMACIÓN DE LA ER

16.1. INFORMACIÓN CONSIDERADA CONFIDENCIAL

La ER de SoftNet mantiene de manera confidencial la siguiente información:

- Material comercialmente reservado de la ER: planes de negocio y diseños e información de propiedad intelectual, e información que pudiera perjudicar la normal realización de sus operaciones.
- Información de los suscriptores y titulares, incluyendo contratos, información que puede permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores y titulares.
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores y titulares.

16.2. INFORMACIÓN QUE PUEDE SER PUBLICADA

- Información respecto de la revocación o suspensión de un certificado, sin revelar la causal que motivó dicha revocación o suspensión, la publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.
- Información de certificados (siempre que el suscriptor lo autorice en el contrato del suscriptor) y su estado.

La publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.

17. RESPONSABILIDADES

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

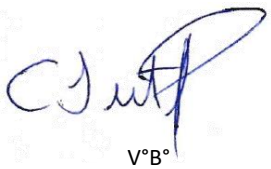
18. CONFORMIDAD

Este documento ha sido aprobado por el Responsable de la ER 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.

19. HISTORIAL DE CAMBIOS

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

Fecha	Versión	Descripción	Autor
01/08/2020	*1.0*	*Documento Inicial*	*Coordinador de Seguridad de la Información*
15/08/2020	*1.0*	*Revisión de Documentos*	*Gerente de Productos y Servicios*
15/08/2020	*1.0*	*Aprobación*	*Representante 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