POLÍTICA DE SEGURIDAD

Firmado Digitalmente por: PEDRO EMILIO RIVERA PEREZ
Fecha: 01/07/2022 14:52:49

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

CONTENIDO

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

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 seguridad de la información 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

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

	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

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

	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.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

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. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La EC de SoftNet tiene como objetivo de seguridad, garantizar la autenticidad e integridad de la información crítica de los procesos de certificación, asegurando que los proveedores de servicios de certificación cumplan con lo establecido en la presente política.

7.1. ORGANIZACIÓN

El Responsable de la EC de SoftNet y el Oficial de Seguridad de la Información son los encargados de velar por el cumplimiento de lo establecido en la presente política.

7.2. GESTIÓN DE RIESGOS

SoftNet exige a sus proveedores de infraestructura la administración de los riesgos relacionados con dicha infraestructura física y de comunicaciones.

7.3. GESTIÓN DE ACTIVOS

SoftNet exige a sus proveedores de infraestructura la protección de los activos críticos de la EC, de acuerdo a la clasificación y controles especificados por el Responsable de Seguridad de la Información de la EC.

7.4. CONTROLES FÍSICOS DE LA INFRAESTRUCTURA TECNOLÓGICA A TRAVÉS DE LA CUAL SOFTNET PRESTA SUS SERVICIOS

emSign PKI, como proveedor de servicio de certificación de SoftNet, cuenta con controles físicos apropiados para lo siguiente:

1. Control de acceso físico al hardware utilizado en conexión con las operaciones de EC.
2. Control de acceso físico sobre el software relevante.
3. Protección contra incendios.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

4. Protección contra fallas de servicios de soporte como energía, telecomunicaciones, etc.
5. Protección contra el robo.
6. Procedimientos de recuperación de desastres.

7.4.1. UBICACIÓN FÍSICA Y CONSTRUCCIÓN

SoftNet realiza sus operaciones de EC desde un centro de datos seguro, el cual es proporcionado por emSign PKI en calidad de su proveedor de servicios de certificación. Dicho cenro de datos cuenta con las siguientes características:

- El centro de datos está equipado con controles físicos y lógicos que hagan que las operaciones de la EC sean inaccesibles para personas no autorizadas.
- El centro de datos es una instalación de hormigón y acero.
- El centro de datos tiene mecanismos de protección de seguridad tales como guardias, cerraduras de puertas.
- El centro de datos es de construcción de piso elevado y una serie de sistemas de seguridad y ambientales resilientes.

7.4.2. ACCESO FÍSICO

La EC de SoftNet se encuentran en un centro de datos seguro proporcionado por el PSC emSign PKI. La entrada a esta instalación segura sólo se permite al personal autorizado y aquel personal autorizado por la seguridad del centro de datos, cuyos movimientos dentro de la instalación se registran y auditan. El acceso físico a esta instalación también se graba en video las 24 horas, los 7 días de la semana. El personal de seguridad in situ supervisa el acceso físico adicional a esta instalación 24/7.

7.4.3. ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

El suministro de energía de la EC de SoftNet, como EC emisora de los sistemas emSign PKI, está protegido con dos fuentes de alimentación mediante el uso de sistemas y generadores de suministro de energía ininterrumpida (UPS) para evitar un apagado anormal en caso de una falla de energía.
Se han implementado sistemas de control climático para garantizar que la temperatura dentro de todas las instalaciones de las EC emisoras de emSign PKI se mantenga dentro de límites operativos razonables.

7.4.4. EXPOSICIÓN AL AGUA

Las instalaciones de la EC de SoftNet, proporcionado por emSign, están ubicadas fuera de cualquier área propensa a inundaciones. Además, se encuentra en un piso superior con pisos elevados, que brindan protección contra la exposición al agua. Además, las paredes exteriores también están selladas para proporcionar protección contra la exposición al agua.

7.4.5. PREVENCIÓN Y PROTECCIÓN DE INCENDIOS

El centro de datos de emSign que aloja la EC de SoftNet, está equipado con un sistema de detección de humo. También está equipado con el sistema de extinción de incendios (FM200) y el dispositivo de detección de humo muy temprano (VESDA) necesarios para la protección contra incendios.

7.4.6. SISTEMA DE ALMACENAMIENTO

Todos los medios magnéticos que contienen información de la EC de SoftNet y que son administrados por eMudhra, incluidos los medios de respaldo, se almacenan en contenedores, gabinetes o cajas fuertes con capacidades de protección contra incendios. Además, se encuentran dentro del área de

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

operaciones del servicio emSign PKI o en un área de almacenamiento segura fuera del sitio y están protegidos contra cualquier acceso físico no autorizado.

7.4.7. ELIMINACIÓN DEL MATERIAL DE ALMACENAMIENTO DE LA INFORMACIÓN

La EC de SoftNet, como EC emisora de emSign PKI, dispone de mecanismos de eliminación de información comercial confidencial o confidencial como se indica a continuación:

- En caso de papel u otro material impreso que contenga dicha información, se triturará o destruirá en un procedimiento generalmente aceptado.
- En el caso de medios magnéticos que contengan elementos confiables de la EC o información comercial confidencial o confidencial, se eliminará de forma segura por daño físico o destrucción completa del activo o mediante el uso de una utilidad aprobada para limpiar o sobrescribir los medios magnéticos;

7.4.8. BACKUP FUERA DE LA INSTALACIÓN

emSign garantiza el empleo de una ubicación fuera del sitio para el almacenamiento y la retención de software y datos de respaldo relacionados con las operaciones de la EC de SoftNet.
El almacenamiento fuera de la instalación:

- Está disponible para personal autorizado las 24 horas del día, los siete días de la semana con el fin de recuperar software y datos.
- Tiene niveles apropiados de seguridad física.
- Se almacenan en cajas fuertes y contenedores resistentes al fuego.

7.5. CONTROLES DE PROCEDIMIENTO

La EC de SoftNet, como EC emisora de emSign PKI, asegura que se adhiere a todos los procesos y procedimientos administrativos detallados en la CP / CPS de emSign PKI los cuales se tratan y describen en detalle en los diversos documentos utilizados dentro y que respaldan a dicho proveedor de servicios de certificación.

7.5.1. ROLES DE CONFIANZA

Se crean roles de confianza en el sistema emSign PKI con el fin de garantizar que una persona que actúe sola no pueda eludir las salvaguardas de seguridad implementadas en el sistema de la EC de SoftNet. Para garantizar esto, las responsabilidades son compartidas por múltiples roles e individuos. Esto se logra creando roles y cuentas separadas en varios componentes del sistema de la EC de SoftNet, y cada rol tiene una capacidad limitada. Este método permite que ocurra un sistema de "controles y equilibrios" entre los diversos roles.
Los roles de confianza dentro del sistema emSign PKI definido incluyen varios roles como Oficial de administración, Oficial de auditoría, Oficial de registro, Oficial de seguridad, Oficial de sistemas, etc. Estos se definen en detalle junto con sus responsabilidades como parte de los documentos de política interna, y pueden ser confidenciales. en naturaleza.

7.5.2. NÚMERO DE PERSONAS REQUERIDAS POR LABOR

emSign asigna al menos dos personas a cada rol de confianza para evitar la posibilidad de un compromiso accidental o intencional de cualquier componente de la infraestructura de la EC de SoftNet. Ésta requiere que al menos dos personas que actúen en un rol confiable tomen medidas que requieran un rol confiable, como activar las claves privadas de la EC emisora, generar un par de claves EC o crear una copia de seguridad de una clave privada EC. Dichas operaciones sensibles también requieren la participación activa y la supervisión de la alta dirección.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

La EC de SoftNet, como EC emisora de emSign PKI, utiliza prácticas comercialmente razonables para garantizar que una persona que actúe sola no pueda eludir las salvaguardas. Utiliza esfuerzos comercialmente razonables para identificar a un individuo separado para cada rol de confianza. Asegura que ningún individuo pueda obtener acceso a ninguna clave privada (que no sea la propia clave privada del individuo).

7.5.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

La EC de SoftNet, como EC emisora de emSign PKI, realiza un procedimiento de detección de seguridad adecuado, incluida la verificación de antecedentes antes de designar a una persona para el puesto de confianza. Cada función descrita aquí se identifica y autentica de manera que se garantice que la persona adecuada tenga la función adecuada para apoyar a la EC.

7.5.4. ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES

La EC de SoftNet hace cumplir la separación de roles para cada una de las funciones y el personal de confianza individual será designado específicamente para las funciones identificadas y definidas en la CP / CPS de emSign PKI y/o como parte de los procedimientos operativos de la EC de SoftNet.
No está permitido que ninguna persona sirva en más de un rol al mismo tiempo, para una actividad o tarea específica.

7.6. GESTIÓN DEL PERSONAL

La EC de SoftNet, como EC emisora de emSign PKI, realiza verificaciones de antecedentes apropiadas de todas las personas seleccionadas para asumir un rol de confianza de acuerdo con el procedimiento de inspección de seguridad designado, antes del comienzo de sus funciones. SoftNet determina la naturaleza y el alcance de cualquier verificación de antecedentes, a su exclusivo criterio.
SoftNet no será responsable de la conducta de los empleados que esté fuera de sus funciones y sobre la cual la EC no tenga control, incluidos, entre otros, actos de espionaje, sabotaje, conducta criminal o interferencia maliciosa.
Todos los empleados, agentes o contratistas independientes que desempeñen funciones de confianza estarán sujetos a estos requisitos de controles de personal.

7.6.1. REQUISITOS SOBRE LA CUALIFICACIÓN, EXPERIENCIA Y CONOCIMIENTO PROFESIONALES

La EC de SoftNet, como EC emisora de emSign PKI, requiere que el personal cumpla con un cierto estándar mínimo con respecto a los antecedentes, calificaciones, experiencia y requisitos de autorización para cada rol confiable. La selección del personal se realiza según este criterio.

7.6.2. PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES

Los procedimientos de verificación de antecedentes incluyen, entre otros, verificaciones y confirmación de:

- Empleo anterior
- Referencias profesionales
- Preparación académica
- Verificación de identidad
- Otros registros gubernamentales relevantes (por ejemplo, identificadores nacionales, etc.)

Cuando no se puedan obtener las verificaciones y confirmaciones debido a una prohibición o limitación de la ley u otras circunstancias, toda EC emisora de emSign PKI utilizará técnicas de investigación sustitutivas disponibles que brinden información similar, incluidas las verificaciones de antecedentes realizadas por agencias gubernamentales y/o privadas aplicables.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

7.6.3. REQUISITOS DE FORMACIÓN

El personal implicado en emSign PKI, incluyendo la EC de SoftNet, seguirán un plan de formación interna adaptada a sus atribuciones asignadas. Esta formación será compatible con las normas de la industria, como las directrices del CA/Browser Forum.

7.6.4. REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN DE FORMACIÓN

Se requieren sesiones de actualización para todo el personal involucrado en el caso del medio ambiente, la tecnología y/o cambios operativos. Los cambios en las prácticas y/o políticas se comunican a todo el personal involucrado.

7.6.5. FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS

No se estipula.

7.6.6. SANCIONES POR ACCIONES NO AUTORIZADAS

En caso que SoftNet o emSign, como su proveedor de servicios certificación+-, detecte una acción no autorizada, emprenderá las acciones disciplinarias necesarias. Cualquier acción que (intencionalmente o no) contraviene la Declaración de Prácticas de Certificación.
Tras la detección de una acción no autorizada, emSIgn iniciará un proceso de investigación. Durante este proceso se evitará que las personas involucradas obtengan acceso a los sistemas e información de emSign.
Las medidas disciplinarias serán tomadas después de la investigación determine la gravedad y la intención de la acción.

7.6.7. REQUISITOS DE CONTRATACIÓN DE TERCEROS

Se requiere que los contratistas externos estén de acuerdo con las Políticas de seguridad de la información de emSign, y el personal temporal no amparado por un acuerdo de confidencialidad existente también estará obligado a firmar el acuerdo de confidencialidad antes de concederse el acceso a los recursos de información.
El acuerdo se examina cuando existen cambios en las condiciones de empleo o contratos.

7.6.8. DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

A todo el personal incorporado dentro de WISeKey se le proporciona el acceso a por lo menos la siguiente información:

- Declaración de Prácticas de Certificación
- Políticas de Certificación
- Política de Privacidad
- Política de Seguridad
- Organigrama y funciones y responsabilidades asignadas
- Procedimientos operacionales
- Procedimientos de respuesta a incidentes

7.6.9. FIN DEL CONTRATO Y PROCEDIMIENTO DE CAMBIO DE ROLES ASIGNADOS

En el caso de que un contrato finalice o se cambie el papel asignado a una persona, emSign se asegura de que se ejecute el procedimiento correspondiente. Este procedimiento incluye al menos los cambios necesarios en los privilegios concedidos a las instalaciones de acceso, sistemas de información y documentación.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

El material asignado (tarjetas inteligentes, ordenadores, etc.) será devuelto o reasignado como sea necesario.
El cambio o terminación será notificado a todas las partes involucradas.

7.7. PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

7.7.1. TIPOS DE EVENTOS REGISTRADOS

El registro de auditoría se mantendrá para:

1. Eventos de EC y Administración del Ciclo de Vida del Certificado:
    a. Se registra la generación, certificación, respaldo, recuperación y / o destrucción de los pares de claves de CA. Esto incluye todos los datos de configuración utilizados en el proceso.
    b. Solicitudes de certificados exitosas y no exitosas, emisiones de certificados, reemisiones de certificados y renovaciones de certificados para certificados de suscriptor. Además, las solicitudes de revocación del Certificado de Suscriptor, incluido el motivo de revocación.
    c. Generaciones y emisiones de CRL.
    d. Custodia de llaves, dispositivos y medios que contienen llaves.
    e. Compromiso de una clave privada.
2. Eventos relacionados con la seguridad:
    a. Actividades de firewall y enrutador.
    b. Cualquier tiempo de inactividad en el sistema, bloqueos de software y fallas de hardware.
    c. Acciones del sistema de CA realizadas por personal de confianza, incluidas actualizaciones de software, reemplazos de hardware y actualizaciones.
    d. Intentos exitosos y fallidos de acceso al sistema PKI.
    e. Eventos del módulo de seguridad de hardware criptográfico, como uso, desinstalación, servicio o reparación y retiro.
    f. Entrada / salida de instalaciones de CA.
    g. Cada movimiento de los medios extraíbles
3. Información de solicitud de certificado:
    a. Toda la documentación e información relacionada proporcionada por el solicitante para el proceso de validación de la solicitud.
    b. Ubicaciones físicas y / o de almacenamiento electrónico de los documentos proporcionados por el solicitante.

Todos los registros incluyen los siguientes elementos:

- Fecha y hora de entrada
- Número de secuencia de entrada
- Descripción de la entrada.
- Identidad de la persona / dispositivo que realiza la entrada del registro

Se generarán y mantendrán los archivos de registro de auditoría para todos los eventos relacionados con la seguridad y los servicios de la CA emisora. Siempre que sea posible, los registros de auditoría de seguridad se generarán automáticamente. Cuando esto no sea posible, se utilizará un libro de registro en papel u otro mecanismo físico. Los registros de auditoría de seguridad de todos los eventos mencionados anteriormente se conservarán y estarán disponibles durante las auditorías de cumplimiento.
El acceso a los sistemas está protegido por Crypto Tokens protegidos con PIN o en forma de nombre de usuario - contraseña, según lo requiera un sistema, software o base de datos específicos. Se

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

garantiza que las contraseñas administrativas en tales casos se dividan, de modo que se requerirá un mínimo de dos personas para realizar una actividad crítica / administrativa.

7.7.2. FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA (LOG)

Los registros de auditoría se verificarán al menos una vez al mes para ver si hay evidencia de actividad maliciosa.

7.7.3. PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA

El período de retención para los registros de auditoría para todas las EC emisoras de emSign PKI será el siguiente:

1. Registros de la actividad de gestión de claves de EC 30 años
2. Registros del sistema de EC de la actividad de gestión de certificados 30 años
3. Sistema operativo registra 7 años
4. Sistema de acceso físico registra 7 años
5. Registros manuales de acceso físico 7 años
6. Grabación de video del acceso a las instalaciones de EC 90 días

7.7.4. PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

En todas las EC emisoras de emSign PKI, los registros de auditoría están protegidos mediante una combinación de controles de acceso físicos y lógicos. Los eventos se registran de manera que no se puedan eliminar ni destruir por ningún período de tiempo que se retengan. Los eventos se registran de manera que se garantice que solo las personas con acceso de confianza autorizado puedan realizar cualquier operación en función de su perfil sin modificar la integridad, la autenticidad y la confidencialidad de los datos.
Los registros de eventos están protegidos de una manera para evitar alteraciones y detectar alteraciones.

7.7.5. PROCEDIMIENTOS DE BACKUP DE LOS REGISTROS DE AUDITORÍA

Todas las EC emisoras de emSign PKI deben realizar diariamente una copia de seguridad in situ de los registros de auditoría generados por el sistema. Al menos una vez al mes, todos los registros de auditoría y resúmenes de auditoría se realizarán en una ubicación segura fuera del sitio. Estos estarán bajo el control de un rol de confianza autorizado. La copia de seguridad del registro de auditoría debe protegerse en el mismo grado que los originales.
Los registros de auditoría están respaldados mediante procedimientos graduales y remotos.

7.7.6. SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

El proceso de auditoría de seguridad de cada EC emisora debe iniciarse al inicio del sistema y puede finalizar solo al apagar el sistema. El sistema de recopilación de auditorías debe garantizar la integridad y disponibilidad de los datos recopilados. Si es necesario, el sistema de recopilación de auditorías debe proteger la confidencialidad de los datos. En el caso de que ocurra un problema durante el proceso de la recopilación de auditoría, las EC emisoras deben determinar si suspender las operaciones de la EC emisora hasta que se solucione el problema.
Los datos de auditoría automatizados se generan y registran a nivel de aplicación, red y sistema operativo. El personal de confianza registra los datos de auditoría generados manualmente.

7.7.7. NOTIFICACIÓN AL SUJETO CAUSA DEL EVENTO

Sin estipulación.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

7.7.8. ANÁLISIS DE VULNERABILIDADES

Todas las EC emisoras de emSign PKI realizarán evaluaciones de vulnerabilidad periódicas. Dichas evaluaciones de vulnerabilidad deberían centrarse en las amenazas internas y externas que podrían dar lugar a acceso no autorizado, manipulación, modificación, alteración o destrucción del proceso de emisión del Certificado.
Las evaluaciones de vulnerabilidad también incluirán el escaneo de la aplicación, así como las pruebas de penetración. Cualquier resultado negativo de dichos informes se someterá a acciones correctivas para dicho resultado negativo. No existirán vulnerabilidades de seguridad comunes en sitios web públicos, alojados en la red.
Los resultados de tales pruebas de evaluación de vulnerabilidad se utilizarán para mejorar la seguridad del medio ambiente.

7.8. ARCHIVO DE REGISTROS

Todas las EC emisoras de emSign PKI deberán mantener un archivo de los registros relevantes según las políticas de retención de registros establecidas en la CP / CPS de emSign y cualquier política de retención de registros que aplique la ley. La EC incluirá detalles suficientes en los registros archivados para mostrar que se emitió un Certificado de conformidad con dicho CP / CPS.

7.8.1. TIPOS DE EVENTOS ARCHIVADOS

Todas las EC emisoras de emSign PKI archivan registros que incluirán toda la evidencia relevante en posesión de la EC emisora, incluyendo:

- Registros de auditoría;
- Solicitudes de certificados digitales y todas las acciones relacionadas;
- Contenido de los certificados digitales emitidos;
- Evidencia de aceptación del Certificado Digital y Acuerdos de Titular del Certificado firmados (electrónicamente o de otro modo);
- Solicitudes de revocación y todas las acciones relacionadas;
- Solicitudes de archivo y recuperación;
- Listas de revocación de certificados digitales publicadas;
- Opiniones de auditoría como se discute en el emSign PKI CP / CPS; y

Para cada Certificado digital, los registros contienen información relacionada con la creación, emisión, uso previsto, revocación y caducidad. Previa solicitud autorizada, la EC pone a disposición documentación relacionada con cada Certificado digital sujeta a la Política de acceso a documentos PKI emSign.

7.8.2. PERIODO DE CONSERVACIÓN

Todas las EC emisoras de emSign PKI archivan y retienen los registros de auditoría de acuerdo con la política de retención de registros de auditoría descrita en la CP / CPS de emSign.

7.8.3. PROTECCIÓN DE ARCHIVOS

Todas las EC emisoras de emSign PKI archivan y protegen los registros de auditoría de acuerdo con la política de protección de registros de auditoría descrita en la CP / CPS de emSign.

7.8.4. PROCEDIMIENTOS DE BACKUP DEL ARCHIVO DE REGISTROS

Todas las EC emisoras de emSign PKI mantienen e implementan procedimientos de copia de seguridad para que las copias de seguridad de los registros archivados se almacenen en una

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

ubicación separada, de modo que en caso de pérdida o destrucción de los archivos primarios esté disponible un conjunto completo de copias de seguridad.

7.8.5. REQUISITOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS

Todas las CA emisoras de emSign PKI marcarán automáticamente sus registros a medida que se creen. Todos los eventos que se registran en la PKI de emSign incluyen la fecha y la hora en que tuvo lugar el evento. Esta fecha y hora se basan en la hora del sistema en la que opera el sistema de CA. emSign PKI utiliza procedimientos para revisar y garantizar que todos los sistemas que operan dentro de emSign PKI se basan en una fuente de tiempo confiable.

7.8.6. SISTEMA DE ARCHIVO DE LA INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

El sistema de recopilación de archivos de emSign PKI es interno.

7.8.7. PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA

Solo los roles y auditores de confianza específicos pueden ver los archivos en su totalidad. La EC emisora puede permitir a los suscriptores obtener una copia de su información archivada. El contenido de los archivos no se divulgará, excepto según lo exija la ley.

7.9. RECUPERACIÓN FRENTE AL COMPROMISO Y DESASTRE

7.9.1. PROCEDIMIENTOS DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES

SoftNet como EC emisora de emSign está obligada a hacer cumplir los controles necesarios para comprobar y demostrar que los procedimientos de gestión de incidentes y vulnerabilidades son eficaces. Las personas involucradas deben ser convenientemente entrenadas en sus roles y responsabilidades en el ejercicio de sus funciones.

7.9.2. ALTERACIÓN DE LOS RECURSOS HARDWARE, SOFTWARE Y/O DATOS

Si los recursos de hardware o de software se ven alterados o se sospecha que han sido alterados, emSign detendrá las operaciones normales hasta que se establezca un entorno seguro. De forma paralela, una auditoría se llevará a cabo con el fin de identificar la causa y disponer las medidas necesarias para evitar futuras repeticiones.
En el caso de que los certificados digitales se emitan durante el periodo de incertidumbre y existe el riesgo de que estos certificados podrían verse comprometidas, a continuación, estos certificados serán revocados y los suscriptores serán notificados de la necesidad de volver a emitir sus certificados.

7.9.3. PROCEDIMIENTO DE ACTUACIÓN ANTE LA VULNERABILIDAD DE LA CLAVE PRIVADA DE UNA AUTORIDAD

En el caso de que una clave privada se vea comprometida en la arquitectura de emSign y además de las estipulaciones en la sección Alteración de los recursos hardware, software y/o datos, las entidades subordinadas en función de la clave privada comprometida serán notificadas de este evento y se llevará a cabo las acciones necesarias.
Todos los certificados emitidos por entidades de subordinación a la clave comprometida desde el momento de compromiso de la clave y la revocación del certificado serán revocados, y las partes involucradas serán notificadas tal como lo dispone la presente CPy DPC. Además, se tomarán medidas para volver a emitir los certificados necesarios.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

7.9.4. CAPACIDAD DE RECUPERACIÓN DESPUÉS DE UN DESASTRE NATURAL U OTRO TIPO DE CATÁSTROFE

El Plan de Recuperación y Desastre de Operaciones de EC está en vigencia con todas las EC bajo emSign PKI, en forma de Plan de Continuidad de Negocio. Este plan cumple el propósito de restaurar las operaciones comerciales centrales cuando las operaciones y / o sistemas se han visto afectados de manera adversa y significativa. Esta restauración se realizará lo más rápido posible. Dicho plan proporcionará la reanudación inmediata de los servicios de revocación en caso de una emergencia inesperada.

El plan de recuperación ante desastres y reanudación comercial es propietario, sensible a la seguridad y confidencial. Por consiguiente, no se pretende que esté disponible de manera general.

Todas las EC emisoras bajo emSign PKI han implementado un plan de compromiso de clave apropiado que detalla las actividades tomadas en caso de compromiso de una clave privada de EC emisora emSign. Dichos planes incluyen procedimientos para:

- Revocación de todos los certificados digitales firmados con la clave privada de esa emSign emisora de EC;
- Notificar a la EC de SoftNet y a todos los titulares de certificados digitales emitidos por dicha EC.

7.9.5. PLAN DE CONTINUIDAD DEL NEGOCIO

El Plan de Continuidad del Negocio es estrictamente confidencial y prevé:

- Procedimientos de compromiso de clave privada, así como procedimientos de revocación de clave pública.
- Procedimientos de manejo de incidentes y compromisos.
- Software, recursos informáticos y / o procedimientos de manejo de datos corruptos.
- Capacidades y procedimientos de continuidad del negocio después de un desastre.

El plan de continuidad del negocio y los planes de seguridad se ponen a disposición de los auditores y se auditan durante los ciclos de auditoría definidos. Estos también están sujetos a pruebas anuales, revisión y actualización de los procedimientos.

7.10. CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

7.10.1. ÁMBITO DE LA INFORMACIÓN CONFIDENCIAL

emSign PKI considera la siguiente información como información confidencial y los protege de la divulgación utilizando un grado razonable de atención:

1. Claves privadas;
2. Datos de activación utilizados para acceder a las claves privadas o para obtener acceso al sistema de CA;
3. Planes de continuidad del negocio, respuesta a incidentes, contingencia y recuperación de desastres;
4. Otras prácticas de seguridad utilizadas para proteger la confidencialidad, integridad o disponibilidad de información;
5. Información mantenida por emSign PKI como información privada de acuerdo con este CP / CPS;
6. Auditoría de registros y registros de archivo; y
7. Registros de transacciones, registros de auditoría financiera y registros de seguimiento de auditoría externa o interna y cualquier informe de auditoría (con la excepción de una carta del auditor que confirme la efectividad de los controles establecidos en este CPS).
8. Cualquier otra información relacionada con el suscriptor o emSign PKI, que puede ser de naturaleza confidencial.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

7.10.2. INFORMACIÓN NO CONFIDENCIAL

Cualquier información que no sea la información indicada como confidencial en este documento se considerará pública. La información adicional que aparece en los certificados y en el repositorio se considera pública.

7.10.3. DEBER DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

Los empleados, agentes y contratistas de emSign PKI están obligados contractualmente a proteger la información confidencial. Además, enSign brinda capacitación a los empleados sobre la protección de la información confidencial.

8. RESPONSABILIDADES

El Responsable de Seguridad de SoftNet 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.

9. CONFORMIDAD

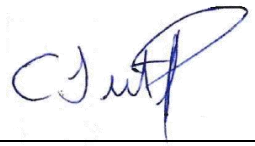
Este documento ha sido aprobado por el Responsable de la EC de SoftNet, y cualquier incumplimiento por parte de los empleados, contratistas y terceros mencionados en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA

10. HISTORIAL DE CAMBIOS

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

Fecha	Version	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 Operaciones*
28/10/2020	*1.0*	*Revision de Documentos*	*Gerente de Productos y Servicios*

Elaborado por:	Revisado por:	Aprobado por:
 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 EC

Prohibido reproducir sin la autorización de la alta dirección
COPIA NO CONTROLADA