SOFTNET

POLÍTICA DE SEGURIDAD

CONTENIDO

1. INTRODUCCIÓN

SOFT & NET SOLUTIONS S.A.C., en adelante SoftNet, es una empresa peruana fundada en el 2007, dedicada a proveer soluciones integrales en alta tecnología con preponderancia en identidad digital, automatización de procesos, facturación electrónica y gestión de proyectos. Como parte de sus planes de expansión en la prestación de servicios, en el año 2020 se constituye como Entidad de Certificación, con lo cual es de las pocas empresas peruanas en brindar todas las variedades de productos y servicios que homologa INDECOPI a través de sus diversos procedimientos de acreditación dentro del marco de la Infraestructura Oficial de Firma Electrónica (IOFE)

2. OBJETIVO

Este documento tiene como objetivo la descripción de operaciones y prácticas de 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

"Según lo indicado en la POLITICA DE CERTIFICACION y DECLARACION DE PRACTICAS - SGEC-PO-01"

4. DEFINICIONES Y ABREVIACIONES

"Según lo indicado en la POLITICA DE CERTIFICACION y DECLARACION DE PRACTICAS - SGEC-PO-01"

5. PARTICIPANTES

"Según lo indicado en la POLITICA DE CERTIFICACION y DECLARACION DE PRACTICAS - SGEC-PO-01"

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.
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 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.
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

"Según lo indicado en la POLITICA DE CERTIFICACION y DECLARACION DE PRACTICAS - SGEC-PO-01"

7.7. PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

"Según lo indicado en la POLITICA DE CERTIFICACION y DECLARACION DE PRACTICAS - SGEC-PO-01"

7.8. ARCHIVO DE REGISTROS

"Según lo indicado en la POLITICA DE CERTIFICACION y DECLARACION DE PRACTICAS - SGEC-PO-01"

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.

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

"Según lo indicado en la POLITICA DE CERTIFICACION y DECLARACION DE PRACTICAS - SGEC-PO-01"

7.9.5. PLAN DE CONTINUIDAD DEL NEGOCIO

"Según lo indicado en la POLITICA DE CERTIFICACION y DECLARACION DE PRACTICAS - SGEC-PO-01"

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.

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.

10. HISTORIAL DE CAMBIOS

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

Fecha	Versión	Descripción	Autor
12/05/2020	*1.0*	*Documento Inicial*	*Coordinador de Seguridad de la Información*
12/05/2020	*1.0*	*Revisión de Documentos*	*Gerente de Operaciones*
28/10/2020	*1.0*	*Revisión de Documentos*	*Gerente de Productos y Servicios*
19/09/2022	*2.0*	*Ajustes en el contenido por repetición de información contenida en la Política de Certificación y Declaración de Practicas SGEC-PO-01 de los capítulos* *3. Objeto De La Acreditación* *4. Definición y Abreviaciones (todo* *5. Participantes (todo)* *7.6 Gestión Del Personal (todo)* *7.7 Procedimientos De Auditoria De Seguridad (todo)* *7.8 Archivo De Registros (Todo) /* *7.9.4. Capacidad De Recuperación Después De Un Desastre Natural U Otro Tipo De Catástrofe /* *7.9.5. Plan De Continuidad Del Negocio* *Estos capítulos tienen la siguiente referencia:**"Según lo indicado en la POLITICA DE CERTIFICACION y DECLARACION DE PRACTICAS - SGEC-PO-01"***	*Gerente del Sistema Integrado de Gestión*
19/09/2022	*2.0*	*Revisión de la modificación*	*Gerente de Productos y Servicios*
19/09/2022	*2.0*	*Aprobación de la versión 2.0*	*Gerente General / Responsable de la EC*
12/06/2023	*2.0*	*Revisión*	*CISO - Gerente SIG*
12/06/2023	*2.0*	*Revisión de Documento*	*Gerente de Productos y Servicios*
12/06/2023	*2.0*	*Aprobación*	*Representante de la EC*
10/06/2024	*2.1*	*Revisión nuevo PSIT*	*CISO - Gerente SIG*
10/06/2024	*2.1*	*Revisión de Documento*	*Jefe PSIT*
10/06/2024	*2.1*	*Aprobación*	*Responsable de la EC*

Fecha	Versión	Descripción	Autor
14/11/2024	*2.1*	*Revisión*	*CISO - Gerente SIG*
14/11/2024	*2.1*	*Revisión de Documento*	*Jefe de Productos Servicios e Infraestructura Tecnológica*
14/11/2024	*2.1*	*Aprobación*	*Responsable de la EC*
01/07/2025	*3.0*	*Revisión y Actualización de Responsable de EC*	*Oficial de Privacidad – CISO GSIG*
01/07/2025	*3.0*	*Revisión*	*Oficial De Seguridad – Jefe de PSIT*
01/07/2025	*3.0*	*Aprobación*	*Responsable de EC – Representante Legal*

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

SOFT & NET Solutions S.A.C. Gerencia

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