POLÍTICA GENERAL DE SEGURIDAD
E-SIGN S.A.

Revisado por:	Aprobado por:
Firmado digitalmente por JUAN CARLOS ARRIAGADA TAPIA Fecha: 2022.06.01 15:47:32 -04'00'	Gonzalo Eugenio Sebastián Yáñez Cárcamo Firmado digitalmente por Gonzalo Eugenio Sebastián Yáñez Cárcamo Fecha: 2022.06.01 08:50:29 -04'00'
Representante de la Dirección	**Gerente General**
Cargo	**Cargo**

Tabla de contenido

Prefacio

Para garantizar un buen funcionamiento, uno de los elementos clave es poder definir una política de seguridad que sea universal para todo el sistema empresa. De esta forma, la operación puede llevarse a través de un método general que permita un ordenado y adecuado uso de los recursos disponibles, sin alterar la calidad y/o confidencialidad que se ha construido con clientes.

En esta dirección es que el aspecto legal y organizacional se unifican, creando así un marco que les permite actuar de forma adecuada interna como externamente.

Dado que esta información es de carácter transversal, todo empleado y profesional que se desempeñe en o con E-Sign debe entender este funcionamiento.

Definiciones

A continuación, se definen algunos conceptos que deben estar claros para dar un cumplimiento apropiado a la presente política:

Activo de información: es todo aquel elemento, sea tangible o no, que contenga datos que sean relevantes para ESign, que se encuentren en formato físico o electrónico, sean equipos o aplicativos, o incluso las personas cuyo conocimiento sirven para los propósitos de la empresa.

Confidencialidad: Es la propiedad de que la información no es puesta a disposición o divulgada terceros no autorizados.

Integridad: Es la propiedad de asegurar la completitud y exactitud de la información.

Disponibilidad: Es la propiedad de estar accesible y usable cuando una entidad autorizada lo solicite.

Seguridad de la Información: Es la preservación de la confidencialidad, integridad y disponibilidad de la información.

Evento de seguridad: Es cualquier situación que indica:

- Una posible violación a la política de seguridad de la información.
- La falta de medidas de protección.
- Una situación previamente desconocida que puede ser relevante para la seguridad.

Incidentes de Seguridad: Se entiende por incidente de seguridad, cualquier evento y/o situación que afecte o vulnere las definiciones y requerimientos de las Políticas y Planes de Seguridad de E-Sign y que por lo tanto pone en riesgo la Seguridad de la Información.

Propósito

a) Esta Política General de Seguridad es un documento vivo, propiedad de E-Sign, que debe ser conocida e interiorizada por toda la organización, por lo tanto, es publicada y difundida al interior de la compañía. Para esto se utilizará el Repositorio Oficial de Documentos (Redmine) al cual tienen acceso todos los empleados de E-Sign.

b) La Seguridad de la Información es el elemento fundamental de la confianza en los sistemas de información, esto se hace aún más importante para el desarrollo y ejecución de las actividades propias de una CA.

c) La Seguridad de la Información permite el intercambio de información de manera segura y confiable, tanto entre personas como también en procesos de negocio.

d) Por lo anterior, para E-SIGN es fundamental mantener y asegurar altos niveles de seguridad y confiabilidad en todos los aspectos de funcionamiento como CA, para esto se utilizan herramientas de Gestión de la Seguridad de la Información, las cuales permiten asegurar altos niveles de confianza e integridad en los procesos necesarios para el funcionamiento de la CA.

e) Esta Política General de Seguridad cuenta con el apoyo y aprobación de la Alta Gerencia y del Comité de Seguridad E-Sign. Sus integrantes manifiestan activamente su adhesión a los objetivos y metas de la Seguridad de la Información y son garantes de su vigencia y cumplimiento. Esto hace responsables del cumplimiento de esta a toda la organización.

Objetivo

El objetivo fundamental de esta Política General de Seguridad de la Información es mantener y reforzar la Seguridad de la Información en todos nuestros procesos e interacciones como CA tanto internamente como también para las partes interesadas. El fin último es mantener seguridad razonable durante la ejecución de todos los procesos críticos de la CA para evitar cualquier tipo de acceso y/o fuga no autorizado de la información. Asimismo, es objetivo de esta política asegurar que se cumplan con todos los requerimientos y normativas legales y contractuales que mantiene E-Sign.

Es por ello que E-Sign asume la responsabilidad de implantar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI) que permita lograr niveles adecuados de seguridad para todos los activos de información, de manera tal de garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Alcance General

Esta Política aplica a todo el personal de E-Sign sin excepción. Esto incluye a:

a) Servicios de “Emisión de certificados de Firma Electrónica”.
b) Todo el Personal de E-Sign (Trusted Employee).
c) Asociados Estratégicos (partners), Proveedores y cualquier tercera parte que por necesidad de negocio accede a los activos de información y/o a las instalaciones de E-Sign y por lo tanto debe cumplir con los objetivos de esta Política General de Seguridad.

Como instrumentos de esta política, E-Sign define una serie de Políticas, Procedimientos y Normas que buscan asegurar el cumplimiento de los objetivos y requerimientos planteados.

Responsabilidades

Todo el personal de E-Sign es responsable de cumplir con los requerimientos de seguridad definidos en esta Política, de la misma forma, todo el personal de E-Sign es responsable de informar/reportar cualquier Incidente de Seguridad, en la ejecución de las actividades diarias propias y de sus

colaboradores, haciendo énfasis en el cumplimiento de las Políticas y Planes de Seguridad. El Oficial de Seguridad es responsable de mantener Políticas y Planes de Seguridad actualizados y vigentes, teniendo en consideración los nuevos riesgos emergentes y las necesidades propias de ESign. Al mismo tiempo es responsable de medir el nivel de cumplimiento al interior de E-Sign mediante un programa regular de auditorías internas.

El Comité de Seguridad es responsable de revisar, autorizar y publicar las actualizaciones a todos los documentos (Políticas y Planes) de Seguridad de E-Sign. También es responsable de evaluar los Incidentes de Seguridad informados y definir los planes de acción necesarios para administrar los riesgos evidenciados. En caso de desviaciones o incumplimientos a las Políticas y Planes de Seguridad, el Comité de Seguridad puede determinar la aplicación de sanciones para la o las personas involucradas. En general, es de responsabilidad del Comité de Seguridad tomar todas las decisiones de alto nivel en materias que incidan en la seguridad de la empresa.

Para brindar una adecuada supervisión sobre los aspectos de seguridad relevantes de E-Sign, el comité de seguridad sesionará – al menos – una vez por mes, en sesiones que serán registradas mediante una Minuta del Comité de Seguridad, las cuales de almacenarán el sistema de información destinado para dicho fin (Redmine).

Requerimientos Legales y Contractuales

a) Leyes de Chile.

b) Ley 19.799, sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma.

c) Decreto N° 181, de 2002, del Ministerio de Economía, Reglamento de la ley 19.799.

d) Auditorías Entidad Acreditadora.

e) Declaración de Prácticas de Certificación (CPS) Vigentes publicadas en nuestro sitio web.

f) SLAs (en la CPS) para con los suscriptores.

Requerimientos de Educación sobre Seguridad

a) Prevenir y minimizar el riesgo de error humano.

b) Asegurar el cumplimiento de los procedimientos y controles internos de la CA.

c) Minimizar la dependencia en las personas críticas y asegurar la segregación de funciones.

d) Difundir el conocimiento de las responsabilidades vinculadas con el ejercicio de la labor.

Prevención y Detección de Virus y otros softwares maliciosos

a) Evitar cualquier tipo de Incidente a la Seguridad de la Información.

b) Evitar la propagación de cualquier tipo de programa maligno, ransomware o virus al interior de la organización.

Administración de la Continuidad del Negocio

a) Mantener y asegurar la integridad del personal de E-Sign ante incidentes de seguridad.

b) Mantener y asegurar la continuidad operativa ante incidentes de seguridad acorde a lo definido en la CPS.

c) Dar cumplimiento a los niveles de servicio establecidos en la CPS.

d) Administrar de manera eficiente los recursos y sistemas necesarios para asegurar el correcto funcionamiento de los procesos críticos de la CA.

e) Restablecer los procesos críticos de la CA ante incidentes naturales que afecten severamente las instalaciones de la CA, según lo establecido en la CPS y DRP.

Las consecuencias de las violaciones a las Políticas y Planes de Seguridad de la Información.

a) Notificaciones, comunicaciones directas, anotaciones en su carpeta de Trusted Employee.

b) Sanciones, amonestaciones, término del contrato, de acuerdo con lo establecido en el Reglamento Interno de E-SIGN, específicamente en su Título XXI “De las sanciones y las multas.

Para asegurar el cumplimiento a los objetivos y requerimientos, E-Sign define Planes de Seguridad específicos para los aspectos fundamentales de Seguridad de la Información:

1) Seguridad del Personal (Política Trusted Employee, Segregación de Funciones, Proceso Contratación, Capacitación Constante en Seguridad).

2) Seguridad de Sistemas de Información (Plan Seguridad Sistemas de Información).

3) Seguridad en las Comunicaciones (Plan de Seguridad Telecomunicaciones).

4) Administración de los Controles Ambientales (Plan de Seguridad Físico).

5) Administración del Riesgo (Evaluación de Riesgo Corporativa – BUSINESS IMPACT ANALYSIS BIA).

6) Administración de la Continuidad Operativa (Plan de Continuidad de Negocios y Recuperación ante desastres - DRP).

Cada uno de los aspectos antes mencionados es abordado en detalle en documentos individuales (Políticas y/o Planes de Seguridad), los cuales establecen con precisión los objetivos individuales de cada aspecto a normar. Finalmente se utilizarán Procedimientos formales, los cuales establecen en detalle la forma y aplicación de cada control necesario para el cumplimiento de los objetivos de las Políticas y Planes de Seguridad y, por lo tanto, de la Política General de Seguridad.

El siguiente diagrama ilustra la relación jerárquica de las Políticas de Seguridad de E-Sign.

La Política General de Seguridad al igual que todos los demás documentos, Políticas y Planes de Seguridad son revisadas:

a) Cada vez que es solicitado por alguna Gerencia.

b) Cuando ocurran incidentes de seguridad que así lo ameriten.

c) Periódicamente, según lo definido por el Comité de Seguridad: esto para asegurar su vigencia, actualización y aplicación constante dentro de la organización.

Todo lo anterior permite asegurar que se administran los riesgos (previstos e imprevistos) de manera adecuada (ordenada y oportuna) acorde a lo definido en la CPS vigentes. Este documento regula las prácticas de certificación de E-Sign y se halla en conformidad con las CP de E-Sign. Todo cambio que se realice a las CPS debe contar con la previa aprobación del Comité de Seguridad.

Incidentes de Seguridad

Se entiende por incidente de seguridad, cualquier evento y/o situación que afecte o vulnere las definiciones y requerimientos de las Políticas y Planes de Seguridad de E-Sign y que por lo tanto pone en riesgo la Seguridad de la Información.

Cualquier incumplimiento y/o desviación sobre lo establecido en la Política General de Seguridad o en los demás documentos de Seguridad será informado y tratado como un "Incidente de Seguridad". Dependiendo de las consecuencias de cada incidente en particular, el comité de Seguridad evaluará la aplicación de sanciones a él o los responsables y definirá las acciones

correctivas que permitan evitar la reincidencia de incidentes ya reportados. Las consecuencias de las violaciones de la política de seguridad son revisadas por el comité de seguridad.

Al mismo tiempo todos los empleados de E-Sign son responsables de reportar cualquier evento e incidente que ponga en riesgo la Seguridad de la Información y por lo tanto el correcto funcionamiento de los procesos críticos de la CA.

Los mecanismos válidos para informar un Incidente de Seguridad son:

a) Correo Electrónico (al Comité de Seguridad y/o Oficial de Seguridad).

b) Telefónicamente (al Oficial de Seguridad).

c) A la Jefatura Directa (por Correo Electrónico o Telefónicamente), quien a su vez deberá escalar al Comité de Seguridad.

d) A través del registro en Redmine ("Reporte Incidente de Seguridad").

Durante sus reuniones calendarizadas, el Comité efectuará la evaluación y revisión de la situación de la Compañía en cuanto a seguridad informática, incluyendo el análisis de incidentes ocurridos y que afecten la seguridad de los procesos críticos de la CA.

La Gerencia de Operaciones es responsable de implementar y velar por el cumplimento de las políticas y procedimientos de seguridad relacionados más estrechamente con la Operación de la CA, todo esto en coordinación con el Comité de Seguridad y el Oficial de Seguridad.

Activos de Información

Activo de Información puede ser descrito como cualquier elemento/objeto que es de valor para la organización, como bases de datos, información de clientes, registros de eventos, contratos, informes, sistemas, documentos (digitales, impresos), entre otros.

Dependiendo de su nivel de importancia los activos de información son clasificados en dos grupos:

a) Activos de Información.

b) Activos de Información Críticos.

Para asegurar la Seguridad de la Información, se definen los activos de información y los activos críticos de información de E-Sign.

El resto de la documentación e información, que no sea categorizada como activo de información, no es objeto de protección por parte de E-Sign y por lo tanto es considerada pública.

Activo de Información Crítico, es toda información que pueda ser leída, replicada, difundida, eliminada; a través de, medios electrónicos o no electrónicos; y en cualquier tipo de medio de almacenamiento volátil o no volátil; y que, a su vez, si llega a estar en manos de personas no indicadas, y si además se da un mal uso, pueda afectar directa o indirectamente a: E-Sign como empresa, trabajadores, clientes, partners y proveedores relacionados.
Los activos críticos de la información son considerados información privada, a la cual sólo puede tener acceso las personas que se hallen autorizadas para ello y requieran dicha información, basado en el principio "need to know".

El acceso a los demás activos de información puede ser restringido por la empresa, de acuerdo con sus necesidades de negocio, a menos que lo impida la ley vigente.

Procesos Críticos de la CA

Los Procesos Críticos de la CA, son todos aquellos que realiza en su calidad de CA, Firma Electrónica Avanzada y Móvil, Sellado de Tiempo y Biometría, para los cuales se comprenden los siguientes puntos:

a) Emisión de Certificados Digitales.

b) Revocación de Certificados Digitales.

c) Publicación en Repositorio Público de Certificados Digitales.

d) Publicación de CRL.

e) Publicación de Servicio de OCSP.

Directrices de Seguridad de la Información

En relación con la Protección de la Información

El Gerente General reconoce que la seguridad de la información es un objetivo institucional, que debe ser impulsado y apoyado por todos los miembros de la organización.

La información es un activo valioso que debe ser protegido de manera consistente con los objetivos institucionales, y los requerimientos legales, normativos y contractuales que sean aplicables.

Se debe tener presente que no es posible eliminar el riesgo, sólo controlarlo, por lo tanto, las medidas que se definan para proteger la información deben ser determinadas en base a un análisis previo que considere el costo beneficio de aplicarlas en relación con los riesgos existentes. El Gerente General de E-Sign debe destinar los recursos necesarios para asegurar que todo el personal reciba entrenamiento permanente en seguridad de la información, de acuerdo con su función y rol en la empresa.

Los riesgos que se identifiquen deberán ser gestionados por la dirección de manera que sean llevados a un nivel aceptable para el negocio. Para esto podrán ser aceptados, eludidos, transferidos o mitigados.

Para aquellos riesgos que no sean aceptables, deberán seleccionarse medidas de protección apropiadas, las cuales serán sometidas a la aprobación de la dirección para asegurar que:

- Son suficientes para llevar el riesgo a un nivel apropiado.
- Tienen un costo apropiado al beneficio que aportan.
- Reciben los recursos y el apoyo necesarios para su implementación.

En relación con la Clasificación de la Información

Los Propietarios de la información deben clasificar la información que esté bajo su responsabilidad en:

- Documentación Publica.
- Documentación Interna.
- Documentación Confidencial.

- Documentación Secreta.

Esta clasificación se realizará en base a la importancia para el buen desempeño de las distintas unidades de E-Sign, y de forma que no ponga en riesgo la Seguridad de la Información de E-Sign S.A. Toda información que no recibe una clasificación debe considerarse como Documentación Interna, de manera que reciba los niveles de protección acordes a esta clasificación.

El Oficial de Seguridad debe preocuparse de que la información reciba una clasificación apropiada, de manera que las medidas de protección que se apliquen corresponden a las necesidades reales institucionales.

Por cada uno de los niveles de clasificación establecidos, se deben definir medidas de protección específicas, las que serán aplicadas por todo el personal.

A continuación, se indica el criterio que debe ser aplicado para clasificar la información y las medidas mínimas para su tratamiento.

Clasificación	Descripción	Tratamiento
Pública	Es toda información que, por su naturaleza, al ser divulgada, no presente riesgos para la seguridad de E-Sign. Normalmente, este tipo de documentación se encuentra publicada en el sitio web de E- Sign. Ejemplos: - Política de Certificados. - Declaración de Prácticas de Certificación. - Política de Precios.	Puede ser entregada y compartida libremente.
Interna	Es toda información, que, por su naturaleza, al ser divulgada, adulterada o destruida, puede generar algún grado de riesgo, o prejuicio, para E-Sign. Ejemplos: - Contratos de trabajo de los colaboradores. - Liquidaciones de sueldo. - Contratos con proveedores. - Información sobre problemas o incidentes de seguridad. - Políticas de Seguridad.	Puede ser accedida por personal de E-Sign S.A., siempre y cuando tenga derechos a acceder a dicha información. Si algún externo requiere información, deberá tener un NDA firmado con E-Sign S.A.

Confidencial	Es toda información que, por su naturaleza, no debe ser divulgada, adulterada o destruida, ya que puede generar prejuicios para E-Sign. Ejemplos: - Balances. - Estados Financieros. - Liquidaciones de Sueldo. - Código Fuente. - Reportes de Auditorías Externas. - Reportes de Auditorías Internas.	Puede ser accedida por personal de E-Sign S.A., siempre y cuando tenga derechos a acceder a dicha información. Si algún externo requiere información, deberá tener un NDA firmado con E-Sign S.A.
Secreta	Es toda información que por su naturaleza no debe ser divulgada ni compartida con terceros, ya que puede representar un riesgo para la seguridad de la información. Ejemplos: - Naming Documents. - Scripts Ceremonias de Llaves. - Claves de Slots de HSM.	Puede ser accedida por personal de E-Sign S.A., siempre y cuando tenga derechos a acceder a dicha información. Si algún externo requiere información, deberá tener un NDA firmado con E-Sign S.A.

Uso de los Activos de Información

Todo uso de activos de información debe ser para propósitos institucionales de acuerdo con las políticas, estándares y procedimientos que se definan y considerando criterios de buen uso.
Los usuarios de activos:

- No se debe divulgar ningún tipo de información de E-Sign o sus clientes que haya sido clasificada como interna, confidencial o secreta, salvo que haya sido expresamente autorizados por el propietario de la información.

- Para el caso de información que sea clasificada como interna, confidencial o secreta, y que se requiera entregar a terceros, la entrega de esta información se realizará posterior a la firma de un acuerdo de confidencialidad con el tercero y aplicando los controles específicos que se definan según el caso.

- Cualquier entrega de información debe cumplir con todos los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo las políticas de seguridad que deberán mantenerse alineadas con la legislación vigente.

- Los terceros que accedan a activos de información de E-Sign, deben mantener elementos de control de acceso a los activos de información.

- Se debe reportar a E-Sign lo antes posible, cualquier incidente que ponga en riesgo la seguridad de la información, para que se tomen las medidas necesarias.

- Queda prohibido la entrega de BD que contenga cualquier tipo de información de clientes a terceros, independiente de que existan acuerdos de confidencialidad de por medio.

Consistencia entre la política de seguridad, la CPS y la CP

La Política de Seguridad de la Información descrita en el presente documento es consistente con lo indicado en las CPS (Declaración de Prácticas de Certificación) y la CP (Política de Certificados) de E-Sign, de cada uno de los servicios de Emisión de certificados, es decir, Firma Electrónica Avanzada y Móvil, Sellado de Tiempo y Biometría.

Difusión

La comunicación de la presente política se efectúa de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, a lo menos se debe hacer difusión mediante los siguientes canales:

- Publicación en sistema Redmine.

- Publicación en el sitio Web de E-SIGN.

- Correo informativo a los interesados.

Revisión de las Políticas

La presente política deberá ser revisada cada tres años o cuando ocurran cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad.

Documentos de Apoyo

Esta Política General de Seguridad está apoyada por documentos adicionales, que complementan y aseguran un manejo adecuado de la Seguridad de la Información, tales como leyes vigentes, normas y estándares.

Preguntas y Actualizaciones

Este documento es actualizado periódicamente, según sea necesario. Por favor envié sus consultas, o cometarios, a comiteseguridad@esign-la.com.

Control de Documento

Versión	Motivo	Fecha	Autor	Revisión
0.1	Creación de borrador de Política	26/08/2011	Luis Donaire	Comité de Seguridad
0.2	Revisión y chequeo de consistencias con Webtrust	27/09/2011	Herman Vega	Comité de Seguridad
0.3	Revisión legal	27/09/2011	Flavio Tapia	Comité de Seguridad
0.4	Correcciones formato	07/12/2011	Luis Donaire	Comité de Seguridad
1.0	Revisión Final	10/04/2012	Luis Donaire	Andrés Cave
1.5	Actualización	12/02/2014	Luis Donaire	Comité de Seguridad
1.6	Actualización y cambio de formato	14/07/2014	Flavio Tapia	Luis Donaire
1.7	Activos de información: aclaración de situación de documentos que no son calificados como activos de información	25/08/2015	Flavio Tapia	Flavio Tapia
2.0	Actualización General de la Política Eliminación de Referencias a Documentación de Symantec Actualización de Responsabilidades Inclusión de Particularidades	Marzo-2019	Luis Chávez	Comité de Seguridad
2.1	Actualización de tipo de documento	Febrero - 2020	Ronald Pérez	Juan Carlos Arriagada
2.2	Actualización del alcance.	Marzo - 2021	Ronald Pérez	Comité de Seguridad
2.3	Actualización de la política que resuelve la No Conformidad levantada en Auditoría de Certificación junio 2021	Octubre 2021	JC Arriagada	Comité de Seguridad
2.4	Se Actualiza el punto “Prevención y Detección de Virus y otros softwares maliciosos”	Mayo 2022	JC Arriagada	Comité de Seguridad