Declaración de Prácticas del Servicio de Valor Añadido (DPSVA)

Servicio de Valor Añadido de Intermediación

Evicertia

Febrero de 2024

Gestión del documento

Nombre e identificación del documento

Este documento declara las prácticas del Servicio de Valor Añadido (SVA) de Evicertia Perú S.A.C, en lo sucesivo Evicertia. El nombre completo del documento es Declaración de Prácticas del SVA (DPSVA) de Evicertia.

Control de cambios

Ver.	Autor	Aprobación	Observaciones
1.0	CSO	Comité de Dirección (14/02/2024)	Se aprueba la primera versión de este documento.

Índice

1 Políticas y documentos aplicables

A continuación, se detallan las políticas y documentos relacionados con los que cumple el Servicio de Valor Añadido (SVA) de Evicertia.

- Ley N.º 27269, Ley de Firmas y Certificados Digitales. Decreto Supremo Nº 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales.
- Ley N.º 29733, Ley de Protección de Datos Personales. Decreto Supremo Nº 003-2013-JUS, Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales.
- ETSI EN 319 401 General Policy Requirements for Trust Service Providers.
- ETSI EN 319 521 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

1.1 Organización que administra los documentos del SVA

Evicertia Perú S.A.C., filial de Evicertia, S.L.U. (empresa del grupo Namirial), es una sociedad mercantil registrada en Perú, especializada en firma electrónica avanzada, notificación fehaciente e identificación digital, y en proporcionar otros servicios electrónicos de valor añadido como Servicio de Intermediación (SI), mediante la explotación de la infraestructura tecnológica de Evicertia, S.L.U. En adelante identificada como “Evicertia”.

Evicertia está reconocida como Prestador de Servicios de Certificación (PSC) en el Registro Oficial de Prestadores de Servicio de Certificación (ROPS) bajo responsabilidad de INDECOPI (que en esta DPSVA se va a identificar como la Autoridad Administrativa Competente (AAC)).

Evicertia, S.L.U. (España), es un PSC, que actúa de acuerdo con lo dispuesto en el Reglamento (UE) 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, así como las normas técnicas del ETSI aplicables a los servicios de confianza, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios. Los servicios de confianza de Evicertia se auditan anualmente de acuerdo con la normativa europea aplicable, bajo lo indicado en las normas ETSI EN 319 401, y ETSI EN 319 521. En adelante identificada como “Evicertia España”.

1.2 Persona de contacto

Los datos adicionales de contacto de Evicertia, son los siguientes:

- Entidad: Evicertia Perú S.A.C.
- Web: https://www.evicertia.com.
- Email: info@evicertia.com.
- Teléfono: + 51 942 094 673.

- Domicilio postal: Calle Dos de Mayo 516, Oficina 406, Miraflores, Lima, Perú.

1.3 Frecuencia de publicación

La información del Prestador del SVA (PSVA), incluyendo la DVPSVA, se publicarán el día siguiente a su aprobación por la AAC. Los cambios en la DVPSVA se rigen por lo establecido en el procedimiento de gestión de este documento y de acuerdo con la normativa de aplicación.

1.4 Publicación y difusión del documento

La presente DPSVA es administrada por Evicertia, y está publicada, para su consulta por cualquier tercero interesado, en su web https://www.evicertia.com/, junto con el resto de documentación relativa a su SVA.

En el sitio web de Evicertia se podrán localizar todas las versiones de todos los documentos públicos relacionados con el SVA de los cuales Evicertia es considerada como PSVA.

El sitio de Evicertia se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de Evicertia, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo de acuerdo con los plazos y procedimientos establecidos con respecto de la continuidad del negocio.

2 Alcance de aplicación del documento

2.1 Participantes

2.1.1 Autoridad de Intermediación

Evicertia es el PSVA en su modalidad de Autoridad de Intermediación (AI) que presta dicho servicio. El servicio es prestado desde la infraestructura de Evicertia España.

2.1.2 Suscriptores del servicio de certificación

Los suscriptores son los usuarios finales de los SVA gestionados por Evicertia. Los suscriptores del servicio pueden ser:

- Personas jurídicas (empresas, entidades, corporaciones u organizaciones) que solicitan a Evicertia (directamente o a través de un tercero) el uso de sus servicios en su ámbito empresarial, corporativo u organizativo.
- Personas físicas que solicitan el servicio para sí mismas.

2.1.3 Partes usuarias

Las partes usuarias son las personas y las organizaciones que reciben la intermediación mediante certificados, firmas electrónicas, sellos de tiempo, o mensajes del PSC.

Como paso previo a confiar en estos mensajes, las partes usuarias deben verificarlos, como se establece en esta DPSVA y/o en las instrucciones disponibles en la página web del PSC.

2.1.4 Emisor y receptor

Los emisores y receptores son las cuentas de correo electrónico y teléfonos móviles, pertenecientes a las partes usuarias, que emiten o reciben mensajes electrónicos cuya entrega sea verificada.

2.1.5 Terceros que confían

Los terceros que confían son las personas físicas o jurídicas que confían en la intermediación mediante certificados, firmas electrónicas, sellos de tiempo, o mensajes de Evicertia, y que han sido emitidos en los términos y condiciones previstas en la presente DPSVA.

2.1.6 Otros

Para la ejecución de los SVA de la presente DPVSA puede que sea necesario, por parte de Evicertia, pactar, contratar o utilizar servicios de terceros para la prestación parcial o total de alguna de sus actividades. En todo momento, en dichas contrataciones se estará a lo indicado en la presente DPSVA.

2.2 Aplicabilidad

El SI no se utilizará para fines distintos de los especificados en el presente documento. Del mismo modo, el servicio deberá emplearse únicamente de acuerdo con la regulación aplicable.

2.3 Conformidad

Evicertia como PSVA se somete a las evaluaciones periódicas obligatorias de la AAC para evidenciar que sus operaciones y controles son conformes con los documentos normativos como la DSPVA.

3 Autoridad de Certificación de Firma, Mensajería y Entrega

3.1 Definición de responsabilidades

3.1.1 Responsabilidades y obligaciones de Evicertia

Evicertia garantiza, bajo su plena responsabilidad, que cumple con la totalidad de los requisitos establecidos en la DPSVA, siendo el responsable del cumplimiento de los procedimientos descritos, de acuerdo con las indicaciones contenidas en este documento.

Evicertia presta los SVA conforme con esta DPSVA.

Evicertia vincula a los suscriptores y terceros que confían en sus SVA, mediante esta DPSVA, en lenguaje escrito y comprensible, con los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en el presente documento.
- Límites de uso de los SVA.
- Información sobre cómo validar un certificado, firmas electrónicas, sellos de tiempo, o mensajes de Evicertia, incluyendo el requisito de comprobar el estado del mismo, y las condiciones en las cuales se puede confiar razonablemente en él, que resulta aplicable cuando el suscriptor actúa como tercero que confía en la intermediación.
- Forma en que se garantiza la responsabilidad patrimonial del Prestador de Servicios de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales el PSVA acepta o excluye su responsabilidad.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.

3.1.2 Responsabilidades y obligaciones del suscriptor

Las obligaciones de los suscriptores con respecto a los SVA de Evicertia son:

- Respetar lo dispuesto en esta DPSVA.
- Formalizar un contrato de prestación de SVA con Evicertia.
- Utilizar los SVA de Evicertia de acuerdo con los procedimientos y, si fuera necesario, los componentes técnicos suministrados por Evicertia, de conformidad con lo que se establece en la DPSVA o en la documentación técnica de Evicertia.
- Notificar cualquier incidente o hecho que afecte a los SVA de Evicertia.

3.1.3 Responsabilidades y obligaciones de los Terceros que confían

Las obligaciones de terceros que confían en los SVA son:

- Cumplir y facilitar el cumplimiento de todo lo estipulado en esta DPSVA, y en sus documentos relacionados.
- El tercero deberá conocer y seguir lo establecido en esta DPSVA y en sus documentos relacionados, siendo de obligado cumplimiento como si del propio PSVA se tratara.
- Verificar los certificados, firmas electrónicas, sellos de tiempo, o mensajes incluyendo la validez del certificado usado en los diferentes SVA de Evicertia.

3.1.4 Limitación de responsabilidad

Evicertia, en la documentación que la vincula con suscriptores y terceros que confían, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

- Evicertia garantiza al suscriptor que los SVA cumplen con todos los requisitos materiales establecidos en esta DPSVA, así como las normas de referencia.

- Evicertia garantiza al tercero que confía en sus SVA que la información contenida o incorporada por referencia en los certificados, firmas electrónicas, sellos de tiempo, o mensajes, excepto cuando se indique lo contrario.
- Evicertia rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en este documento.
- Evicertia limita su responsabilidad a la prestación de los SVA, los cuáles se regularán por el contrato oportuno.
- Evicertia no será responsable de ningún daño directo y/o por terceros como consecuencia del uso indebido de los SVA.
- Evicertia incluye en esta DPSVA cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.
- Evicertia establece, en el contrato con el suscriptor y/o en sus documentos relacionados que la ley aplicable a la prestación de los SVA, incluyendo DPSVA, es la Ley de la República del Perú.

3.1.5 Resolución de disputas

Como se ha indicado en el apartado “Responsabilidades y obligaciones de Evicertia”, Evicertia establece en el contrato con el suscriptor los procedimientos para la resolución de conflictos. En caso de discrepancia entre las partes, las partes intentarán la previa resolución amistosa. A tal fin, las partes deberán dirigir una comunicación a Evicertia por cualquier medio que deje constancia a la dirección de contacto indicada en este documento.

Si las partes no alcanzaran un acuerdo al respecto, cualquiera de ellas podrá someter el conflicto a la jurisdicción civil, de conformidad con las normas aplicables.

3.2 Gestión del ciclo de vida de las claves

Evicertia emplea sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

3.2.1 Generación de las claves del servicio

El PSVA se asegurará de crear las claves criptográficas del servicio en un entorno seguro y totalmente controlado.

Para la generación de las claves se han seguido los procedimientos de ceremonia de claves de Evicertia, dentro del perímetro de alta seguridad destinado a esta tarea.

- Las actividades realizadas durante la ceremonia de generación de claves han sido registradas, fechadas y firmadas por todos los individuos participantes en la misma. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado determinado por Evicertia.
- Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.

Para la generación de la clave del certificado del SVA se utilizan dispositivos con las certificaciones *Common Criteria EAL4+*, que tienen un nivel igual o superior a *FIPS 140-2 level 3*.

Los certificados del SVA han sido generados por los prestadores:

- Bit4ID S.A.C. (RUC Nro. 20555049464) (en adelante Bit4ID) siguiendo lo indicado en su Declaración de Prácticas de Certificación, encontrándose disponibles en la página web: https://web.uanataca.com/pe/. Los certificados son de 2.048 bits y una duración de hasta 2 años.
- CAMERFIRMA PERÚ, S.A.C. (RUC No. 20566302447) (en adelante Camerfirma) siguiendo lo indicado en su Declaración de Prácticas de Certificación, encontrándose disponibles en la página web: https://www.camerfirma.com.pe/. Los certificados son de 2.048 bits y una duración de hasta 2 años.

3.2.2 Protección de la clave privada

El PSVA se asegurará de custodiar de manera segura la clave privada del servicio, conservando la misma únicamente dentro de los dispositivos criptográficos donde se han generado (*Common Criteria EAL4+*), y mediante los procedimientos indicados por el fabricante de dicho dispositivo.

Evicertia realiza copias de backup de las claves privadas de los certificados, de tal manera que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de estas. Tanto la generación de la copia como la recuperación de ésta necesitan al menos de la participación de dos personas, y siempre siguiendo los procedimientos del fabricante del dispositivo criptográfico.

Estos ficheros de recuperación se almacenan en armarios ignífugos y en el centro de custodia alternativo.

3.2.3 Distribución de la clave pública

Los certificados de Evicertia son comunicados a los terceros que confían, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en la web de Evicertia.

Los usuarios pueden acceder al depósito para obtener las claves públicas.

El certificado de las Autoridades de Certificación Raíz y Subordinadas estarán a disposición de los usuarios en la página web del Prestador de Servicios de Certificación que ha generado los certificados de Evicertia.

3.2.4 Re-emisión de la clave

Los algoritmos utilizados para la generación de las claves y certificados están de acuerdo con lo indicado en la norma ETSI TS 119 312.

Las claves se re-emitirán cuando los algoritmos utilizados se consideren débiles y ETSI recomiende su renovación.

Los certificados se renovarán, por lo menos, con un mes de antelación a su expiración.

3.2.5 Término del ciclo de vida de la clave privada

Para la destrucción de las claves privadas se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente de tal manera que no se puedan volver a utilizar.

Con anterioridad a la destrucción de las claves, se solicitará la revocación del certificado de las claves públicas asociadas a las mismas.

Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de Evicertia. Para el reinicio se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.

Finalmente se destruirán de forma segura las copias de seguridad.

3.3 Ciclo de vida del módulo criptográfico

El PSVA realizará ejecutará los procedimientos técnicos necesarios para confirmar la seguridad del ciclo de vida del hardware (que cumplirá con la certificación *Common Criteria EAL4+*) utilizado para el SVA, en particular:

- Evicertia asegura que el hardware criptográfico usado para el SVA no se ha manipulado durante su transporte mediante la inspección del material entregado.
- El hardware del módulo criptográfico no ha sido manipulado durante su almacenamiento.
- Los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.
- Las claves privadas del servicio se generan directamente en los módulos criptográficos de Evicertia donde se almacenan cifradas.
- La activación y duplicación de dichas claves en el hardware del módulo criptográfico se ha realizado por personal que ocupa roles de confianza, mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, usando al menos un control de acceso de dos personas en un ambiente físico seguro.
- La gestión de acceso a las claves privadas de los certificados del SVA se realiza según los controles establecidos por el HSM donde se custodian.
- El hardware de firma funciona correctamente.
- Para la desactivación de las claves privadas de Evicertia se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.
- Las claves de firma del SVA que son almacenadas en un módulo criptográfico son borradas antes de que el dispositivo sea retirado.
- En el apartado “Término del ciclo de vida de la clave privada del SVA” se indica que para la destrucción de las claves privadas se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente de tal manera que no se puedan volver a utilizar.

3.4 Servicio de Certificación de Firma, Mensajería y Entrega

3.4.1 Acceso al servicio

El acceso a las diferentes URL del servicio de entrega cualificada siempre se realizará mediante protocolos seguros y comunicaciones cifradas.

3.4.2 Autenticación del emisor

La autenticación del emisor para enviar comunicaciones se hará mediante usuario (vinculando a su correo electrónico) y contraseña, proveyendo el servicio medio para aplicar políticas complejas de contraseñas y reseteo seguros de las mismas.

3.4.3 Autenticación del receptor

La autenticación del receptor se realiza mediante doble factor de autenticación con una URL temporal aleatoria, y un OTP (*One-Time Password*) que será enviado al email o teléfono móvil del receptor.

3.4.4 Eventos y evidencias

El Servicio de Certificación de Firma, Mensajería y Entrega es un servicio que permite transmitir datos entre partes terceras por medios electrónicos y aporta pruebas relacionadas con la gestión de los datos transmitidos, incluida la prueba del envío y la recepción de los datos, y que protege los datos transmitidos frente a los riesgos de pérdida, robo, deterioro o alteración no autorizada, por lo tanto el servicio de Evicertia permite recopilar evidencias que permitan asegurar que los mensajes electrónicos del emisor son entregados al receptor de los mismos garantizando la integridad de la evidencia y la veracidad de la misma.

El encargado de garantizar esta integridad y veracidad es el propio PSC, a través de una serie de procesos criptográficos como la aplicación de firmas electrónicas y sellos de tiempo. Tanto los procesos de firma como los sellos de tiempo son proporcionados por PSC dados de alta en el ROPS.

Las evidencias en Evicertia se denominan *affidavits* y son documentos en los que se recopila toda la información pericial que permita demostrar que un evento se ha producido, y no ha sido modificado con posterioridad. En los *affidavits* se puede encontrar:

- Datos de información del emisor y receptor de los mensajes electrónicos.
- El contenido emitido, junto con los documentos adjuntos procesados, además se incorporan resúmenes criptográficos de los mismos.
- En los *affidavits* se puede encontrar información sobre los siguientes eventos:
    - Envío y emisión al servidor de correo del destinatario.
    - Entrega al servidor de correo del destinatario o fallo si no se pudiera entregar.
    - Apertura del mensaje.
    - O acciones posteriores del receptor (si es que se producen).
    - La referencia temporal estará indicada en horario *Coordinated Universal Time* (UTC).

Cada affidavit es firmado electrónicamente por el servicio, y se le incluye un sello de tiempo cualificado, para de esta manera garantizar la integridad del documento y que éste no haya sido modificado con posterioridad.

El emisor tendrá acceso a todos sus *affidavits* en el servicio de entrega cualificada, durante el periodo de custodia contratado con un periodo mínimo de quince años. El receptor podrá acceder a los *affidavits* a través del servicio de soporte o por información del emisor. Una vez que el periodo de vigencia contratado haya concluido ninguna de las partes tendrá acceso a los *affidavits*.

En el caso de producirse un fallo con la integridad de los *affidavits*, o se produjera cualquier incidencia asociada a la integridad del contenido durante el proceso de entrega se comunicará desde el servicio de soporte de Evicertia a las partes interesadas.

3.5 Sincronización del reloj con el UTC

Todos los dispositivos utilizados por Evicertia están sincronizados mediante protocolo NTP (*Network Time Protocol)* a través de internet (*RFC 1305 Network Time Protocol*), utilizando alguno de los siguientes servidores *NTP stratum 1*: pool.ntp.org, pudiéndose configurar otros como ntp.roa.es, u hora.rediris.es.

3.6 Gestión de la seguridad

3.6.1 Organización de la seguridad de la información

Evicertia como PSVA ha implementado un Sistema de Gestión de la Seguridad de la Información (SGSI) que tiene como alcance todos los servicios del SVA. Dicho SGSI está certificado y es auditado anualmente por auditores externos a la organización.

La gestión de la seguridad depende directamente de la Dirección de Evicertia a través del Comité de Seguridad y Riesgos Tecnológicos y el Comité de Riesgos Jurídicos y de Cumplimiento, liderado por el CISO global para todo el grupo Evicertia.

3.6.2 Política de seguridad de la información

Evicertia cuenta con una política de seguridad que se puede consultar en la web (https://www.evicertia.com/), y que ha sido comunicada tanto internamente como externamente a cualesquiera terceros interesados. El alcance de la política de seguridad cubre todas las operaciones del SVA de Evicertia.

3.6.3 Gestión de riesgos

Evicertia realiza de manera periódica un análisis de riesgos para todos los activos de la organización, entre los que están incluidos los activos del SVA de la presente DPVSA. En dicho análisis se evalúan los activos, las amenazas que tienes y el impacto que se generaría si una amenaza se materializa sobre un activo.

Una vez evaluado el riesgo, el CISO presenta los resultados de este al comité de seguridad, y se determinan las salvaguardas que se deben de implementar para aceptar, reducir o transferir los riesgos detectados.

3.6.4 Documentación

Evicertia, como parte de lo requerido en su SGSI, tiene documentado, versionados y publicados internamente todos los procedimientos operativos y de seguridad del SVA.

3.6.5 Seguridad en el trato con terceros

Evicertia exige medidas de seguridad equivalentes a cualquier tercero o proveedor externo implicado en las labores del SVA. Adicionalmente, todos los terceros que presten servicios son auditados por el equipo de seguridad de Evicertia.

3.6.6 Clasificación y gestión de activos

Evicertia mantiene un inventario de activos donde están recogidos todos los activos de la compañía incluyendo también los que forman parte del SVA. El inventario de activos depende directamente del análisis y gestión de riesgos del SGSI, y sobre dicho activo se han establecido la clasificación de seguridad en base a sus requisitos de Autenticación, Confidencialidad, Integridad, Disponibilidad y Auditorías, documentando las reglas del control de acceso.

3.6.7 Seguridad del personal

Requisitos de historial, calificaciones, experiencia y autorización

Todo el personal está cualificado y/o ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

El personal en puestos de confianza no tiene intereses personales que entren en conflicto con el desarrollo de la función que tenga encomendada.

En general, Evicertia retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de conflictos de interés y/o la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.

Evicertia no asignará un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por una falta que afecte su idoneidad para el puesto. Por este motivo, previamente se realiza una investigación hasta donde permita la legislación aplicable, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales.
- Referencias profesionales.

Procedimientos de investigación de historial

Evicertia, antes de contratar a una persona o de que ésta acceda al puesto de trabajo, realiza las siguientes comprobaciones:

- Referencias de los trabajos de los últimos años
- Referencias profesionales
- Estudios, incluyendo titulación alegada.

Evicertia obtiene el consentimiento inequívoco del afectado para dicha investigación previa, y procesa y protege todos sus datos personales en cumplimiento de la normativa vigente en materia de protección de datos personales.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente aplicable. Los motivos que pueden dar lugar a rechazar al candidato a un puesto fiable son los siguientes:

- Falsedades en la solicitud de trabajo, realizadas por el candidato.
- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato.

Requisitos de formación

Evicertia forma al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, manteniendo archivo de dicha formación.

Los programas de formación son revisados periódicamente, y son actualizados para su mejora y mejorados de forma periódica.

La formación incluye, al menos, los siguientes contenidos:

- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad de Evicertia. Uso y operación de maquinaria y aplicaciones instaladas.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

Requisitos y frecuencia de actualización formativa

Evicertia, actualiza la formación del personal de acuerdo con las necesidades, y con la frecuencia suficiente para cumplir sus funciones de forma competente y satisfactoria, especialmente cuando se realicen modificaciones sustanciales en las tareas de certificación.

Sanciones para acciones no autorizadas

Evicertia dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, adecuado a la legislación laboral aplicable.

Las acciones disciplinarias incluyen la suspensión, separación de las funciones y hasta el despido de la persona responsable de la acción dañina, de forma proporcionada a la gravedad de la acción no autorizada.

Requisitos de contratación de profesionales

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados por Evicertia. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían, una vez evaluados, dar lugar al cese del contrato laboral.

En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la DPSVA, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, no obstante, lo cual, el PSVA será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación del SVA por tercero distinto a Evicertia.

Suministro de documentación al personal

El PSVA suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de realizar su trabajo de forma competente y satisfactoria.

3.6.8 Seguridad física y del entorno

Controles de seguridad física

Evicertia ha establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, y los equipamientos empleados para las operaciones para la prestación del SVA.

En concreto, la política de seguridad de Evicertia aplicable a los SVA establece prescripciones sobre lo siguiente:

- Controles de acceso físico.
- Protección frente a desastres naturales.
- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Protección antirrobo.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

Estas medidas resultan aplicables a las instalaciones desde donde se presta el SVA, en sus entornos de producción y contingencia, las cuales son auditadas periódicamente de acuerdo con la normativa aplicable y a las políticas propias de Evicertia destinadas a este fin.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia las 24 horas siguientes al aviso.

Localización y construcción de las instalaciones

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta y está ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

Las salas donde se realizan las operaciones criptográficas en el Centro de Proceso de Datos (CPD) cuenta con redundancia en sus infraestructuras, así como varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.

Acceso físico

Evicertia dispone de tres niveles de seguridad física en el CPD (entrada del Edificio donde se ubica, acceso a la sala del CPD y acceso al Rack), debiendo accederse desde los niveles inferiores a los niveles superiores.

El acceso físico a las dependencias de Evicertia donde se opera el SVA está limitado y protegido mediante una combinación de medidas físicas y procedimentales. Así:

- Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro de este.
- El acceso a las salas se realiza con lectores de tarjeta de identificación y/o cerraduras electrónicas, gestionado por un sistema informático que mantiene un log de entradas y salidas automático.
- Para el acceso a la sala donde se ubican los procesos criptográficos es necesario la autorización previa de Evicertia a los administradores del servicio de *colocation* que disponen de la llave para abrir la sala y la jaula, pero no los armarios.

Electricidad y aire acondicionado

Las instalaciones del CPD de Evicertia disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado.

Exposición al agua

Las instalaciones están ubicadas en una zona de bajo riesgo de inundación. Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

Prevención y protección de incendios

Las instalaciones y activos del CPD de Evicertia cuentan con sistemas automáticos de detección y extinción de incendios.

Almacenamiento de soportes

Únicamente el personal autorizado tiene acceso a los medios de almacenamiento. La información de más alto nivel de clasificación se guarda en una caja de seguridad fuera de las instalaciones del CPD.

Tratamiento de residuos

La eliminación de soportes, tanto papel como magnéticos, se realizan mediante mecanismos que garantizan la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se desechan en cuyo caso se destruyen físicamente, o se reutilizan previo proceso de borrado permanente o formateo. En el caso de documentación en papel, mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

Copia de respaldo fuera de las instalaciones

Evicertia utiliza un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que son independientes del CPD.

3.6.9 Gestión de operaciones

Evicertia garantiza que sus sistemas se operan de forma segura, para lo cual ha establecido e implantado procedimientos para las funciones que afectan a la provisión de su SVA.

El personal al servicio de Evicertia ejecuta los procedimientos administrativos, operacionales y de gestión de acuerdo con la política de seguridad.

Funciones fiables

Evicertia ha identificado, de acuerdo con su política de seguridad, las siguientes funciones o roles con la condición de fiables:

- **Administrador de Sistemas**: responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación
- **Auditor Interno**: responsable de proporcionar aseguramiento del cumplimiento de los procedimientos operativos por parte de sus responsables. Se trata de una persona externa al departamento de Sistemas de Información. Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.
- **Custodio**: responsable de custodiar las tarjetas criptográficas donde se almacena la clave precompartida bajo el modelo de seguridad n de m. Esta función es compatible con el resto de las funciones de esta DPC.
- **Oficial de verificación de identidad**: responsable de asegurar los procesos de verificación de la identidad de los suscriptores de alguno de los servicios de confianza de Evicertia, como puede ser el de entrega cualificada.
- **Operador de Sistema**s: responsable necesario juntamente con el Administrador de Sistemas del funcionamiento correcto del hardware y software soporte de la plataforma de certificación. El operador es responsable de los procedimientos de copia de respaldo y mantenimiento de las operaciones diarias de los sistemas
- **Propietario de producto:** encargado de coordinar, controlar y gestionar los equipos y entregables de los desarrollos de confianza de Evicertia. Debe encargarse de las tareas de

triaje de errores y funcionalidades, y será el responsable de desplegarlos en los diferentes entornos.

- **Responsable de Seguridad**: encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de Evicertia. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos. Adicionalmente, Evicertia implementa criterios en sus políticas para la segregación de las funciones, como medida de prevención de actividades fraudulentas.

Identificación y autenticación para cada función

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurará que cada persona realiza las operaciones para las que está asignado.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante usuario/contraseña, certificado digital, tarjeta de acceso físico y/o llaves.

Roles que requieren separación de tareas

Las funciones fiables se establecen bajo el principio del mínimo privilegio, garantizado una segregación de funciones, de modo que la persona que ostente un rol no tenga un control total o especialmente amplio de todas las funciones de certificación, asegurando el debido control y vigilancia, limitando así cualquier tipo de comportamiento fraudulento a nivel interno.

La concesión del mínimo privilegio para las funciones de confianza, se hará teniendo en cuenta el mejor desarrollo de la actividad y será lo más limitado posible, considerando la estructura organizativa de Evicertia en cada momento.

3.6.10 Manejo de medios y seguridad

Evicertia garantiza que todos los medios son operados de manera segura de conformidad con lo establecido en la política de seguridad, y la clasificación de la información los mismos, implantando procedimientos que cubran todo el ciclo de vida de dichos medios en Evicertia, teniendo especial cuidado en la reutilización y destrucción de estos cuando ya no sean necesarios.

3.6.11 Planificación del sistema

El departamento de atención al cliente de Evicertia mantiene un registro de las capacidades de los equipos. Juntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

3.6.12 Reportes de incidentes, informes de seguimiento y solución

Evicertia dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos.

En el documento de seguridad de Evicertia se desarrolla en detalle el proceso de gestión de incidencias.

Evicertia tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

3.6.13 Seguridad en redes

Evicertia protege el acceso físico a los dispositivos de gestión de red, y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad, creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se transfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos TLS o del sistema VPN con autenticación por doble factor.

3.6.14 Monitoreo

Evicertia tiene montados varios sistemas de monitorización interna y externa que alertan en caso de pérdida de disponibilidad del servicio. Las alertas de monitorización están integradas con los sistemas de gestión de tickets de Evicertia generando los tickets necesarios en el caso de producirse una disrupción en el servicio siendo enviadas al servicio de atención al cliente 24h x 7d, que en base a la alerta producida ejecutarán el procedimiento correspondiente, o en su defecto escalarán al segundo nivel de soporte para su resolución dentro de los tiempos comprometidos de SLA con los suscriptores.

Adicionalmente, los servicios de monitorización interna tienen configurados diferentes chequeos que van desde la monitorización de la capacidad del SVA, la revisión del control de acceso, la integridad de ficheros y procesos, y varios miles de chequeos adicionales que como en el caso anterior y en base a su criticidad provocan diversos tipos de alertas.

3.6.15 Intercambio de datos y software

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de Evicertia.

Los análisis de vulnerabilidad deben ser ejecutados, repasados y revisados por medio de un examen de estos acontecimientos monitorizados. Estos análisis deben ser ejecutados periódicamente de acuerdo con el procedimiento interno que está previsto para este fin.

Los datos de auditoría de los sistemas son almacenados con el fin de ser utilizados en la investigación de cualquier incidencia y localizar vulnerabilidades.

3.6.16 Gestión de accesos a los sistemas

Evicertia realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.

En particular:

- Se dispone de controles basados en firewalls en alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.
- Evicertia dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- Evicertia dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.
- Cada persona tiene asociado un rol para realizar las operaciones de certificación.
- El personal de Evicertia es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

3.6.17 Archivo

Período de conservación de registros

Evicertia archiva los registros especificados anteriormente durante al menos 15 años, o el período que establezca la legislación vigente.

El archivo de información estará disponible para su consulta por un auditor cualificado en función del cumplimiento de la legislación vigente.

Protección del archivo

Evicertia protege el archivo de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo. El archivo está protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable.

Evicertia asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en instalaciones seguras externas.

Procedimientos de copia de respaldo

Evicertia dispone de un centro de almacenamiento externo del CPD principal para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido sólo para personal autorizado.

Evicertia como mínimo realiza copias de respaldo diarias de todos sus documentos electrónicos para casos de recuperación de datos.

Requisitos de sellado de fecha y hora

Los registros están fechados con una fuente fiable vía NTP. No es necesario que esta información se encuentre firmada digitalmente.

Localización del sistema de archivo

Evicertia dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

Procedimientos de obtención y verificación de información de archivo

Evicertia dispone de un procedimiento donde se describe el proceso para verificar que la información archivada es correcta y accesible. Evicertia proporciona la información y medios de verificación al auditor.

3.6.18 Desarrollo y mantenimiento

Las aplicaciones son desarrolladas o implementadas por Evicertia de acuerdo con estándares de desarrollo y control de cambios.

Las aplicaciones disponen de métodos para la verificación de la integridad y autenticidad, así como de la corrección de la versión a emplear.

3.6.19 Control de cambios

Evicertia ha aprobado un control de cambios que contiene los procedimientos necesarios para realizar cualquier cambio o modificación del SVA, gestionando los mismos en base a la criticidad del cambio a implementar.

3.7 Compromiso de los servicios de intermediación

Procedimientos de gestión de incidencias y compromisos

Evicertia ha desarrollado políticas de seguridad y continuidad del negocio que le permiten la gestión y recuperación de los sistemas en caso de incidentes y compromiso de sus operaciones.

Corrupción de recursos, aplicaciones o datos

Cuando acontezca un evento de corrupción de recursos, aplicaciones o datos, se seguirán los procedimientos de gestión oportunos de acuerdo con las políticas de seguridad y gestión de incidentes de Evicertia, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres de Evicertia.

Compromiso de las claves privadas de la entidad

En caso de sospecha o conocimiento del compromiso de Evicertia, se activarán los procedimientos de compromiso de claves de acuerdo con las políticas de seguridad, gestión de incidencias y continuidad del negocio, que permita la recuperación de los sistemas críticos, si fuera necesario en un centro de datos alternativo.

Continuidad del negocio después de un desastre

Evicertia restablecerá los servicios críticos de acuerdo con el plan de incidencias y continuidad de negocio existente restaurando la operación normal de los servicios anteriores en las 24 horas siguientes al desastre.

3.8 Término de la organización que administra el SVA

Evicertia asegura que las posibles interrupciones a los suscriptores de los servicios y a terceras partes sean mínimas como consecuencia del cese de los servicios del prestador de servicios de certificación. En este sentido, Evicertia garantiza un mantenimiento continuo de los registros definidos y por el tiempo establecido de acuerdo con la presente DPSVA.

No obstante, lo anterior, si procede, Evicertia ejecutará todas las acciones que sean necesarias para transferir a un tercero o un depósito notarial, las obligaciones de mantenimiento de los registros especificados durante el periodo correspondiente según esta DPSVA o la previsión legal que corresponda.

Antes de terminar sus servicios, Evicertia desarrollará un plan de terminación, con las siguientes provisiones:

- Proveerá de los fondos necesarios, incluyendo un seguro de responsabilidad civil, para continuar la finalización de las actividades de revocación.
- Informará a todos los suscriptores del servicio, terceros que confían y en general cualquier otro con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 2 meses.
- Transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios.
- Destruirá o deshabilitará para su uso las claves privadas encargadas del SVA.
- Ejecutará las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos durante los períodos de tiempo respectivos.
- Comunicará a la Autoridad Administrativa Competente, con una antelación mínima de 2 meses, el cese de su actividad.
- Asimismo, le comunicará la apertura de cualquier proceso concursal que se siga contra Evicertia, así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.

3.9 Registros de información concerniente a la operación

Evicertia produce y guarda registro, al menos, de los siguientes eventos relacionados con la seguridad del servicio:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.

- Intentos de accesos no autorizados a los sistemas que dan soporte al SVA..
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones.
- Encendido y apagado de las aplicaciones del SVA.
- Cambios en los detalles del SVA y/o sus claves.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de éste.
- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor, en caso de certificados individuales, o de la persona física identificada en el certificado, en caso de certificados de organización.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte al servicio.
- Eventos relativos a la sincronización y recalibración del reloj.

Las entradas del registro incluyen los siguientes elementos:

- Fecha y hora de la entrada.
- Número de serie o secuencia de la entrada, en los registros automáticos.
- Identidad de la entidad que entra el registro.
- Tipo de entrada.

Frecuencia de tratamiento de registros de auditoría

Evicertia revisa sus logs cuando se produce una alerta del sistema motivada por la existencia de algún incidente.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.

Evicertia mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de logs.
- Que los ficheros de logs no se reescriben.
- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.

- Los ficheros de logs se guardarán en ficheros estructurados susceptibles de incorporarse en una BBDD para su posterior exploración.

Protección de los registros de auditoría

Los ficheros de registro de auditoría se protegen mediante controles físicos y lógicos de acceso, lecturas, modificaciones, borrados no autorizados.

El acceso a los ficheros de logs está reservado sólo a las personas autorizadas. Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de logs de auditoría.

Procedimientos de copia de respaldo

Evicertia dispone de un procedimiento adecuado de copia de seguridad de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

Localización del sistema de acumulación de registros de auditoría

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo, las comunicaciones de red y por el software de los servicios de confianza, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado. Todo ello compone el sistema de acumulación de registros de auditoría.

Notificación del evento de auditoría al causante del evento

Cuando el sistema de acumulación de registros de auditoría registra un evento, no es preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

3.10 Auditoría

3.10.1 Frecuencia de la auditoría de conformidad

Evicertia llevará a cabo auditorías de conformidad según lo que indique la AAC y por lo menos de manera anual, además de las auditorías internas que realiza bajo su propio criterio o en cualquier momento, debido a una sospecha de incumplimiento de alguna medida de seguridad.

3.10.2 Auditoría de registros y archivos

La auditoría verifica respecto a Evicertia:

- Que la entidad tiene un sistema de gestión que garantice la calidad del servicio prestado.
- Que la entidad cumple con los requerimientos de la DPSVA.
- Que la DPSVA y demás documentación jurídica vinculada, se ajusta a lo acordado por Evicertia y con lo establecido en la normativa vigente.
- Que la entidad gestione de forma adecuada sus sistemas de información.
- La validez de los registros generados.
- La existencia y validez del archivo.

3.10.3 Auditor

Las auditorías se realizarán por auditores externos autorizados por la AAC, y serán siempre independientes al PSVA, y con las limitaciones que la AAC considere oportunas.

3.11 Otros aspectos legales de la operación del SVA

3.11.1 Tarifas y políticas de reembolso

Evicertia puede establecer una tarifa o una política de reembolso por el uso de su SVA, de la que, en su caso, se informará oportunamente a los suscriptores.

3.11.2 Cobertura de seguro de responsabilidad civil

Evicertia dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional, que mantiene de acuerdo con la normativa vigente aplicable.

3.11.3 Información confidencial y/o privada

Evicertia mantendrá de manera confidencial la siguiente información:

- Material comercialmente reservado como PSVA, de los suscriptores de la empresa y de los terceros que confían, incluyendo términos contractuales, planes de negocio y propiedad intelectual;
- Información que pueda permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores de empresa y los terceros que confían;
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares o terceros que confían.
- Cualquier otra información que pudiera perjudicar la normal realización de sus operaciones.

Evicertia considerará como información privada, la siguiente:

- De conformidad con lo establecido por la Norma Marco sobre privacidad del APEC, se considera información personal, cualquier información relativa a un individuo identificado o identificable.
- Información que pueda permitir a personas no autorizadas la construcción de un perfil de las actividades de los usuarios de los servicios de certificación.
- En todos los casos, deberá ser suscrita por el mismo, su consentimiento para el tratamiento y almacenamiento de estos datos.

3.11.4 Información no privada

Los certificados de firma utilizados en el servicio del SVA estarán publicados en su página web.

3.11.5 Derechos de Propiedad intelectual

Evicertia establece en el contrato con el suscriptor las cláusulas contractuales de obligaciones y derechos relacionados a la propiedad intelectual.

3.11.6 Notificaciones y comunicaciones entre participantes

Evicertia establece en el contrato con el suscriptor las cláusulas por el cual las partes se podrán notificar hechos mutuamente.

3.11.7 Conformidad con la Ley aplicable

Evicertia establece en el contrato con el suscriptor las cláusulas de conformidad con la ley aplicable, indicando que la ley aplicable a la prestación del SVA, incluyendo esta DPSVA, es la Ley de la República del Perú.

3.11.8 Exención de garantías

Evicertia, en la documentación que la vincula con suscriptores y terceros que confían, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

Evicertia garantiza al suscriptor que el SVA cumple con todos los requisitos materiales establecidos en esta DPSVA, así como las normas de referencia.

Evicertia garantiza al tercero que confía en su SVA que la información contenida o incorporada por referencia en el sello es correcta, excepto cuando se indique lo contrario.

Evicertia rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en este documento.

3.11.9 Indemnizaciones

Evicertia establece en el contrato con el suscriptor las cláusulas aplicables en caso de indemnización.

3.11.10 Fuerza mayor

Evicertia establece en el contrato con el suscriptor las cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

4 Anexo I: acrónimos

A continuación de muestra una lista de los acrónimos utilizados en el presente documento:

- AAC: Autoridad Administrativa Competente.
- AI: Autoridad de Intermediación.
- CC: *Common Criteria.*
- CSO: *Chief Security Officer.*
- CPD: Centro de Proceso de Datos.
- CRL: *Certificate Revocation List.*

- DPSVA: Declaración de Prácticas del Servicio de Valor Añadido.
- EAL: *Evaluation Assurance Leve*ls.
- ESI: *Electronic Signatures and Infrastructures*.
- ETSI: *European Telecommunications Standards Institute*.
- FIPS: *Federal Information Processing Standard*.
- HSM: *Hardware Secure Module*.
- HTTP: *Hypertext Transfer Protocol*.
- INDECOPI: Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual.
- NTP: *Network Time Protocol*.
- OCSP: Online Certificate Status Protocol.
- OTP: *One-Time Password*.
- PSC: Prestador de Servicios de Certificación.
- PSVA: Prestador del Servicio de Valor Añadido.
- ROPS: Registro Oficial de Prestadores de Servicio de Certificación.
- RSA: *Rivest–Shamir–Adleman* (criptosistema de clave pública).
- RFC: *Request For Comments*.
- RUC: Registro Único de Contribuyentes.
- SAC: Sociedad Anónima Cerrada.
- SGSI: Sistema de Gestión de la Seguridad de la Información.
- SLA: *Service Level Agreement* (Acuerdo de nivel de servicio).
- SI: Servicio de Intermediación.
- SVA: Servicio de Valor Añadido.
- TLS: *Transport Layer Security*.
- UE: Unión Europea.
- URL: *Uniform Resource Locator*.
- UTC: *Coordinated Universal Time*
- VPN: *Virtual Private Network*.